Proyecto Fin de Carrera

(*Ingeniería Técnica de Telecomunicaciones: Sistemas de Telecomunicación*)

ANÁLISIS DE TEXTOS CIFRADOS DE LOS SIGLOS XVI Y XVII

Autora: SARA GÓMEZ HERNÁNDEZ

Tutores: JOSÉ MARÍA DE FUENTES GARCÍA-ROMERO DE TEJADA

DIEGO NAVARRO BONILLA

Diciembre 2010

RESUMEN

La función esencial de la criptografía es mantener la privacidad de la comunicación, de forma que el mensaje sea inteligible tan solo para sus destinatarios. Esta necesidad de ocultar cierta información ha estado siempre presente en la vida del ser humano, datando el primer sistema criptográfico del que se tiene constancia del siglo V a.C.

En este proyecto, además del análisis exhaustivo de varios sistemas concretos, se realiza un recorrido a través de la historia de esta disciplina desde sus comienzos hasta el siglo XVII, época a la que pertenecen los documentos analizados.

Se han estudiado varios sistemas de cifrado de la comunicación utilizados en los siglos XVI y XVII. El estudio se ha basado fundamentalmente en dos textos de relevancia histórica de dichos siglos. El objetivo ha sido tratar de averiguar de qué tipo de sistemas se trata y analizar ciertas características de cada uno de ellos para llegar a ciertas conclusiones básicas para su futuro desciframiento. Para ello se han debido realizar ciertas transformaciones sobre los textos codificados, obtener varios parámetros estadísticos a través de la herramienta Cryptool, realizar comparaciones con textos en claro de la época y plantear diversas hipótesis. En base a este estudio analítico y a los resultados en él obtenidos se plantearán varias líneas futuras de investigación.

ÍNDICE

ÍNDICE DE FIGURAS

CAPÍTULO 1

INTRODUCCIÓN

1. INTRODUCCIÓN

La criptografía se define como el arte de escribir con clave secreta o de un modo enigmático (1). El principio fundamental de la criptografía es conservar la privacidad de la comunicación entre emisor y destinatario cambiando el mensaje original de forma que tan solo sea comprensible para aquella persona o personas a las que está destinado. La palabra criptografía es de origen griego y significa literalmente "escritura oculta". El cifrado es la conversión del texto original en un mensaje cifrado, al que se denomina criptograma. El descifrado es la operación inversa, por la que se recupera el texto original. Los pasos necesarios siguen un conjunto de reglas conocidas por el emisor y el destinatario de dicho mensaje, que pueden incluir o no una clave. El conjunto de métodos destinados a recuperar la clave utilizada por los interlocutores, a fin de obtener el texto original se llama criptoanálisis.

A lo largo de la historia el ser humano ha sentido la necesidad de comunicarse y, hoy más que nunca, de esconder de alguna manera la información confidencial, personal o de cualquier otra índole que se nos pueda ocurrir, pues el simple hecho de poseer esa información puede reportar cierto poder sobre los demás. Por desgracia son los conflictos bélicos los que provocan la mayor parte de estos adelantos técnico-científicos, o los que de alguna manera agudizan el ingenio humano para conseguir sus propósitos. La criptografía no es una excepción; como se puede apreciar a continuación, la mayoría de los sistemas criptográficos fueron creados en tiempos de guerra.

1.1. CRIPTOGRAFÍA CLÁSICA

Debido a la época a la que pertenecen los textos analizados en este proyecto, dejaremos aparte las tendencias actuales en criptografía, puesto que no serían de gran ayuda a la hora de estudiar documentos creados y cifrados 3 y 4 siglos antes. Nos centraremos en la criptografía clásica, describiendo las diferentes formas en las que el ser humano ha encriptado la información confidencial, desde tiempos remotos (siglos antes de Cristo) hasta bien entrado el siglo XVII.

1.1.1. Historia Antigua

En este apartado se detallan los principales métodos de criptografía utilizados desde los orígenes de la disciplina hasta principios del siglo XV.

- **La escítala (siglo V a.C.)**

El primer caso evidente de utilización de métodos criptográficos se produjo durante la guerra entre Esparta y Atenas, por parte de los lacedemonios. Este cifrado se basaba en la modificación del mensaje original incluyendo símbolos innecesarios que desaparecían al enrollar el mensaje en un rodillo llamado escítala, de longitud y grosor preestablecidos. Aun conociendo la técnica utilizada, si no se disponía de las dimensiones exactas de la escítala, sería muy difícil para un posible interceptor del mensaje llevar a cabo su criptoanálisis. La longitud y el grosor de la escítala eran la clave del sistema: (2)

Figura 1. Escítala

- **El cifrador de Polybios (siglo II a.C.)**

Es el cifrador por sustitución más antiguo que se conoce. El método se basaba en una tabla secreta, en cuyos ejes se ponían diferentes combinaciones de letras o números y dentro de la tabla las letras del alfabeto. Cada letra del mensaje a cifrar era sustituida por sus “coordenadas”, por lo que duplica el tamaño del texto en claro. (3) Se ve bastante más claro en el siguiente ejemplo: (4)

	A	B	C	D	E
A	a	b	c	d	e
B	f	g	h	i/j	k
C	l	m	n	o	p
D	q	r	s	t	u
E	v	w	x	y	z

Figura 2. Cifrador de Polybios (4)

Mensaje	P	O	L	Y	B	I	O	S	E	S	E	L	R	E	Y
Criptograma	CE	CD	CA	ED	AB	BD	CD	DC	AE	DC	AE	CA	DB	AE	ED

- **Cifrado de César (siglo I a.C.)**

El cifrado César, también llamado cifrado por desplazamiento, desplazamiento de César o código de César, es una técnica de codificación muy simple y una de las más utilizadas. Se trata de un cifrado por sustitución en el que cada letra del texto original es sustituida por otra letra que se encuentra un determinado número de posiciones más adelante en el mismo alfabeto. Por ejemplo, con un desplazamiento de 3, la A sería sustituida por la D (situada 3 lugares a la derecha de la A), la B sería reemplazada por la E, etc. El método recibe este nombre porque Julio César lo usaba en la comunicación con sus generales.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Figura 3. Alfabeto de cifrado del César para castellano módulo 27

Mensaje	C	I	F	R	A	D	O	C	E	S	A	R
Criptograma	F	L	I	U	D	G	R	F	H	V	D	U

Al periodo de tiempo que transcurre entre el siglo I a.C. y el siglo XV de nuestra era, se le denomina "edad oscura" Durante este tiempo la criptografía se considera magia negra y gran parte del conocimiento que se tenía hasta entonces se pierde. Por otra parte, la disciplina empieza a florecer en Persia.

En el año 855 aparece en Arabia el primer libro sobre criptografía. Al-Kindi muestra de manera orgullosa en su libro un mensaje griego descifrado que era deseado por el emperador bizantino. Su criptoanálisis se ha basado en un análisis de frecuencia ayudado con el conocimiento de una pequeña porción del comienzo del texto original; este mismo criptoanálisis es el que se empleará en la Segunda Guerra Mundial contra Enigma, que acaparó la mayor atención de cuantas máquinas han existido y existen en la actualidad. (5)

En 1379 el papa Clemente VII huye a Aviñón y ordena que su secretario, Gabrieli di Lavinde (Parma), diseñe un código nuevo para cifrar sus mensajes. Dicho código consistía en una combinación de palabras codificadas y sustituciones de letras individuales. Gabrieli creó una lista con las palabras más comunes que serían sustituidas por combinaciones de dos letras y el resto de palabras que no estaban presentes en la lista se cifrarían por sustitución monoalfabética. Este código tan se utilizaría a lo largo de los próximos 450 años, especialmente en los círculos diplomáticos.

En 1412 se escribe en Arabia una enciclopedia con 14 tomos en donde se explican conceptos de criptografía. En ella se explican las técnicas de sustitución y transposición y sustitución. La transposición consiste en la reordenación de los caracteres que conforman el texto original, de manera que el criptograma contenga los mismos caracteres pero en distinta posición, impidiendo así la comprensión del texto. En la técnica de sustitución los caracteres son reemplazados por otros diferentes. Se explica también en esta enciclopedia un método consistente en repetidas sustituciones de cada carácter del texto claro. Es la primera vez en la historia que habla de un método como éste. (6)

Aquí termina lo que hemos denominado historia antigua de la criptografía.

1.1.2. Historia de la Criptografía en los siglos XV, XVI y XVII

En el siglo XV tiene lugar en Italia un auge de la criptografía debido a un gran desarrollo de la vida diplomática.

- **Siglo XV**

1466: León Battista Alberti, pintor, músico, arquitecto y escritor, concibe el primer sistema polialfabético, que se define como aquel en que se utilizan varios cifrados monoalfabéticos, que son periódicamente reutilizados. Para ello emplea varios abecedarios, alternando entre uno y otro cada tres o cuatro palabras. El emisor y el destinatario debían fijar la posición de dos círculos concéntricos, que determinarían la correspondencia de los símbolos.

En uno de los discos se representaban los diferentes abecedarios usados en este método, y el otro disco se rellenaba con el abecedario tradicional, más los números 1, 2, 3 y 4. Según la posición del disco interior, se definen 24 posibles sustituciones.

Una vez fijada la correspondencia entre los caracteres de los discos interior y exterior, cada una de las letras del texto en claro del disco exterior es sustituida por las correspondientes letras del disco interior, pasando al abecedario correspondiente (preestablecido por emisor y receptor) cada *X* palabras; este parámetro *X* también debía ser fijado por los comunicantes.

Figura 4. Disco de Alberti (5)

Alberti era el secretario de una institución oficial que pertenecía a la corte papal; dicha institución se encargaba únicamente de tareas relacionadas con la criptografía. Por todo ello a Alberti se le conocerá como el "padre de la criptografía". (7)

Se citan a continuación algunas de las máquinas, algo más complicadas que el disco de Alberti, puesto que son posteriores al mismo. Estas máquinas siguen un sistema propio de cifrado polialfabético.

- **Siglo XVI** (6)

1518: Se imprime el primer libro sobre criptografía cuyo título es "Polygraphia libri sex", escrito por el abad Johannes **Trithemius** en lengua alemana. En este libro también se describen cifrados polialfabéticos con las nuevas tablas de sustitución rectangulares.

1563: Giovanni Battista **Porta** publica "De Furtivis Literarum Notis", un libro en el que describe distintos métodos de cifrado y criptoanálisis. En él se menciona el primer cifrado por sustitución digráfica.

A finales del S. XVI Francia toma la delantera en criptoanálisis.

1577: El brillante criptoanalista flamenco **Van Marnix** cambia el rumbo de la historia europea al descifrar una carta española en donde se explicaban los planes para conquistar Inglaterra enviando tropas desde los Países Bajos.

1585: El diplomático francés Blaise de Vigenère publica su libro "Tractié de Chiffre" en donde presenta el primer sistema polialfabético con autoclave, conocido como "Le chiffre indéchiffrable" aunque más adelante se le cambiará el nombre por el de **el cifrado de Vigenère**. Este método será de especial relevancia en el posterior estudio de los textos analizados.

La idea de la autoclave perdurará en el tiempo y se aplicará en los algoritmos futuros como el DES en los modos CBC y CFB.

El sistema de cifrado de Vigenère es un sistema polialfabético o de sustitución múltiple, de clave privada o secreta. Este tipo de criptosistemas aparecieron para sustituir a los monoalfabéticos o de sustitución simple, basados en el Algoritmo de Cesar que hemos visto anteriormente, en los que cada letra del texto era reemplazada por otra, que presentaban ciertas debilidades frente al ataque de los criptoanalistas relativas a la frecuencia de aparición de elementos del alfabeto. El principal elemento de este sistema es la llamada Tabla de Vigenère, una matriz de caracteres cuadrada, que se muestra a continuación:

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figura 5. Tabla de Vigenére (8)

Para el proceso del cifrado, el mensaje a cifrar en texto claro ha de descomponerse en bloques de elementos (letras), del mismo tamaño de la clave y aplicar sucesivamente la clave empleada a cada uno de estos bloques, utilizando la tabla anteriormente proporcionada, perteneciendo las letras de la clave a la columna de la izquierda.

Un ejemplo podría ser el siguiente, utilizando como clave la palabra *ejemplo* y como mensaje en claro *cifrado de Vigenère*

Mensaje	C	I	F	R	A	D	O	D	E	V	I	G	E	N	E	R	E
Clave	E	J	E	M	P	L	O	E	J	E	M	P	L	O	E	J	E
Criptograma	G	R	J	D	P	O	C	H	N	Z	U	V	P	B	I	A	I

Este sistema de cifrado polialfabético fue considerado invulnerable hasta que en el S.XIX se descifraron algunos mensajes que habían sido codificados con este sistema, a través del análisis de la repetición de bloques de caracteres: la distancia entre cada bloque y su repetición suele ser múltiplo de la palabra que se ha utilizado como clave.

1586: Se intenta llevar a cabo el complot Babington por el cual se asesinaría a la reina Elisabeth I de Inglaterra y se colocaría en el trono a Mary Stuart, Reina de Escocia. El "Servicio Secreto Británico" pone fin a esta trama y consigue los nombres de los conspiradores, condenando a Mary Stuart.

Mary se comunicaba a través de cartas con sus conspiradores. Pero el mensajero, que era un espía de Elisabeth realizaba copias exactas de cada carta y las enviaba a Francis Walsingham, secretario del estado de Elisabeth, que a través de Thomas **Phelippes** consiguió descifrarlas revelando el complot.

Pero la cosa no quedó ahí, Walsingham quería saber la identidad de los conspiradores por lo que hizo que Phelippes añadiera una posdata a una carta, de manera que en la respuesta a la carta, Mary incluyó el nombre de los implicados.

- **Siglo XVII**

En el S. XVII comienza la época de las **cámaras negras**. La mayoría de los gobiernos cuentan con departamentos donde profesionales de la disciplina se encargan de romper los criptosistemas que van recibiendo.

1623: Sir Francis **Bacon** describe un sistema de esteganografía por el que cada letra del texto original es sustituida por un bloque de cinco letras formado por una combinación de las letras 'A' y 'B' que son intercaladas en un texto normal con una fuente distinta. Este método es el precursor del que posteriormente se conocerá como codificación binaria de 5 bits.

1628: Antoine **Rissignol** se convierte en el primer criptoanalista contratado a tiempo completo tras descifrar un mensaje del enemigo gracias al cual se puso fin al sitio que los hugonotes ejercían sobre Realmont. Desde entonces, el papel del criptoanalista ha sido fundamental en toda organización militar.

No se detalla en la memoria la historia de la criptografía a partir del siglo XVIII puesto que no es relevante para el análisis de los textos que son estudiados en este proyecto, que datan de los siglos XVI y XVII.

1.2. CRIPTOGRAFÍA EN ESPAÑA

En España, la utilización de la Criptografía en el ámbito político se observa por primera vez en la Corona de Aragón, a mediados del siglo XV. Después se va prodigando bajo el reinado de los Reyes Católicos y es ya imprescindible cuando España se convierte en un imperio, con Carlos I. Los primeros criptosistemas que se emplearon eran sustituciones que cambiaban el texto pleno por números romanos. Los cifrados resultantes eran confusos y a menudo no podían ser interpretados por el legítimo receptor. Pronto se abandonaron y se comenzó a usar el nomenclátor, que fue el único sistema utilizado a partir del siglo XVI. Se trataba de un catálogo en el que aparecían sustituciones de letras, palabras y grupos de palabras por distintos signos. Los

nomenclátores de Carlos I fueron muy simples y fácilmente rotos por los italianos y por Philibert Babou, criptoanalista del rey francés Francisco I. Cuando en 1556 Felipe II subió al trono, sabedor de la ineficacia de las cifras españolas, mandó cambiarlas. Es precisamente durante el reinado de Felipe II cuando más se ha utilizado la Criptografía en nuestro país.

Conspiración, sabotaje, intriga y asesinato eran moneda corriente en la vida política de la segunda mitad del siglo XVI, caracterizada, además, por el uso interesado de la propaganda, una manipulación que, en cierto modo, recuerda a la guerra fría del siglo XX. Esta situación marcó las relaciones entre los distintos Estados europeos, creando en el marco de la política internacional un clima de recelo y secretismo. El engaño era práctica habitual y ningún Estado podía confiar en la lealtad de sus amigos. Sobre todo si representaba a la primera potencia mundial del momento.

Felipe II era consciente de esta situación y de la importancia decisiva que tenía el control de la información para mantener la supremacía imperial de España. Por eso dedicó gran cantidad de recursos económicos y humanos a los servicios secretos, conformando la red de espionaje más compleja, mejor organizada y con mayor presencia efectiva de la época. Experto en el arte de la criptografía, su carácter desconfiado y su tendencia natural al secreto lo convertían en el perfecto dirigente de las labores de inteligencia: reglamentaba el uso de los textos cifrados, coordinaba la información y su posterior transmisión a través de los correos, decidía la contratación de espías y controlaba la distribución de los «gastos secretos», alternando las labores propias de su reinado con las de un verdadero jefe del servicio de espionaje.

Felipe II usó diversos nomenclátores. Por un lado estaba la llamada **cifra general**, que era la usada regularmente para comunicar con las embajadas en los diferentes países. Se cambiaba cada cuatro años. Por otra parte, estaban las distintas cifras particulares que se empleaban con cada uno de los ministros y virreyes de las colonias americanas. En el apéndice se muestra la cifra particular empleada en 1568 en la comunicación con el duque de Alba.

Los nomenclátores usados por Felipe II contienen ya un número importante de sustituciones, con objeto de elevar la seguridad mostrada por otros de épocas anteriores.

Puede observarse que el mostrado en el anexo de la memoria incluye homófonos para las vocales, signos para los bigramas y trigramas más frecuentes, una amplia lista de palabras de uso común y una regla que indica como insertar nulos en los textos cifrados. Sin embargo, los nomenclátores de Felipe II también presentaban descuidos en su diseño que facilitaban su criptoanálisis. Por ejemplo, en el nomenclátor de 1557 mostrado en el anexo, el modo de cifrar los bigramas compromete claramente su seguridad: cada bigrama compuesto por una consonante y una vocal se cifra con el mismo signo y con una marca alrededor de dicho signo en función de la vocal, lo que supone una debilidad. Se deberían haber utilizado signos totalmente distintos para cada uno de estos bigramas. Una observación similar puede hacerse en los trigramas. También hubiese sido conveniente emplear homófonos para las consonantes frecuentes.

No obstante, a pesar de sus deficiencias, los nomenclátores de Felipe II eran los más seguros de su época. No era fácil su criptoanálisis con texto cifrado únicamente; aunque hubo quienes lo hicieron. Uno de ellos fue el francés François Viète, más conocido como matemático que como criptoanalista. Viète resolvió varios nomenclátores usados por Felipe II; entre ellos, el que empleó el rey en 1589 para comunicarse con Alejandro Farnes, duque de Parma, que comandaba las tropas españolas de la Santa Liga contra el rey francés Enrique IV, aunque tardó seis meses en hacerlo. Cuenta la historia que Felipe II, enterado de la ruptura de sus cifras por Viète y creyendo que estas eran indescifrables, supuso que el matemático galo debía emplear la brujería en el criptoanálisis y solicitó al Papa su excomunión. Naturalmente, el Pontífice no atendió esta petición; pero no por considerar absurda la existencia de la magia negra, sino porque sabía que las cifras españolas podían romperse sin recurrir a la brujería, ya que así lo estaba haciendo su criptoanalista Giovanni Battista Argenti. (9)

Por la importancia de la Cifra General de Felipe II dentro de la historia de la criptografía española, nos detendremos un poco más en ella.

1.2.1. La *Cifra General* de Felipe II

El 24 de mayo de 1556, con apenas un año de reinado, el emperador español Felipe II escribió una carta a su tío Fernando I (emperador del Sacro Imperio y Rey de Hungría) su decisión de cambiar las cifras usadas durante el reinado de su padre Carlos

V, por haber caído en desuso o estar comprometidas. Seis meses después, la primera Cifra General del reinado de Felipe II entró en vigor.

La *Cifra General* era usada para las comunicaciones del Emperador con los principales miembros de su gobierno en el extranjero. Podemos considerarla como una clave diplomática maestra. La *Cifra General* de 1556 tuvo los siguientes destinatarios:

- la Serenísima Princesa de Portugal, gobernadora de España
- el Duque de Saboya, gobernador de Flandes
- los Virreyes de Nápoles, Sicilia y Cataluña
- el Cardenal de Trento
- el Marqués de Pescara en Milán
- el Cardenal de Burgos en Sena
- el Príncipe Andrea Doria
- los embajadores en Roma, Venecia, Génova, Francia e Inglaterra.

La Cifra General de 1556 está datada en Gante, a 8 de Noviembre de 1556, y según David Kahn, fue uno de los mejores sistemas de su tiempo. Se compone de tres partes: un vocabulario de sustitución monoalfabética con homófonos (donde cada letra podía ser sustituido por un signo, a escoger entre varios); un silabario (para cifrar grupos de dos o tres letras); y un diccionario de términos comunes. (10)
La Cifra General original se guarda en el Archivo de Simancas. La copia que se presenta en el anexo de esta memoria está sacada de la compilación de J.P. Devos. (11)

La Cifra General de Felipe II solamente se mantuvo secreta durante unos tres meses. En Febrero de 1557, el secretario papal Triphon Bencio consiguió romper el cifrado de una carta enviada al Cardenal de Burgos Francisco Pacecco en Siena; Pacecco[1] fue uno de los usuarios de la Cifra General. A partir de ahí, el criptoanalista consiguió reconstruir parte de la Cifra.

[1] (http://www.cripto.es/museo/felipeii-1556.htm (NOTA: Según esta página el primero en romper la cifra general fue Triphon Benicio. Apenas existen referencias sobre esto y las pocas que hay parecen ser todas de la misma fuente. Por el contrario, son numerosas las referencias que apuntan a Viète como el que logró descifrarlo.))

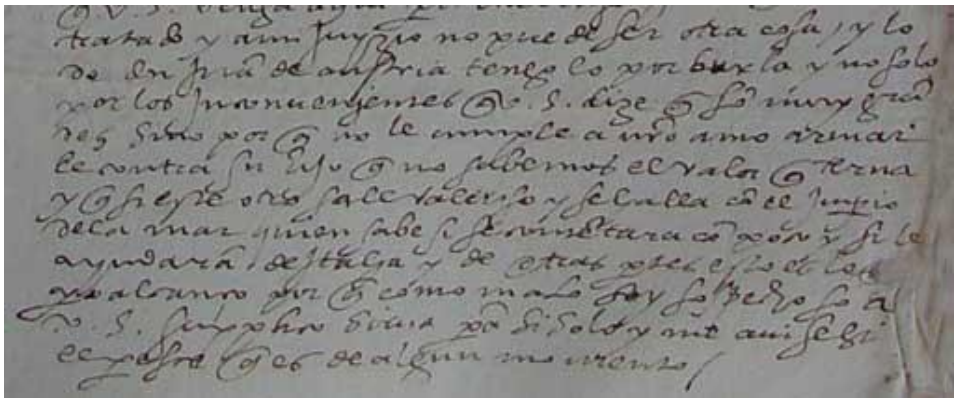


Figura 6. Carta manuscrita de Felipe II

Famoso es el caso de la máquina Enigma que codificaba los mensajes de los alemanes y que trajo de cabeza a los aliados hasta que estos fueron capaces de "romper" la clave. Pues algo parecido a los alemanes, salvando las distancias, le ocurrió 400 años antes a Felipe II cuando su sistema de codificación de mensajes secretos, llamado La Cifra General y que el soberano creía indescifrable, fue "reventado".

Aunque en esta ocasión no lo descifró una máquina como en la II Guerra Mundial, ni tampoco fue por medio de la magia negra como creía Felipe II, sino que fue un hombre, un matemático francés llamado François Viéte.

Conocida es la manía de Felipe II por la discreción y el secretismo y no en vano su red de espías, cuyos oídos abarcaban desde las Filipinas a las Américas pasando por Europa, era tan temida por sus enemigos como podían serlo los Tercios. Por eso, para comunicarse con los miembros de su gobierno en el extranjero, el rey usaba en sus cartas La Cifra General, un complicado sistema de codificación considerado por los expertos como uno de los mejores de su tiempo.

Felipe II comenzó a sospechar cuando, algunas veces, sus enemigos se adelantaban a sus planes de un modo casi premonitorio, aunque confiado en lo inviolable de su clave la continuó usando hasta 1590, año en que se le despejaron todas las dudas. En ese año, el rey francés Enrique IV, hizo pública una carta codificada de un miembro del gobierno español dirigida a Felipe II donde se detallaba la trama para desplazar a Enrique IV del trono. El rey español no daba crédito a que persona humana hubiera sido capaz de descifrarla por lo que sólo podía haberse conseguido por medio de

la magia negra y la hechicería. Por este motivo, Felipe II no dudó en quejarse de ello ante el Papa. El padre Feijoo cuenta así lo sucedido.

> ***Habiéndose interceptado en Francia, cuando ardían las guerras de la Liga, algunas cartas de España, escritas con caracteres voluntarios, en que se añadía la precaución de variar diferentes alfabetos dentro de una misma carta, lo que parece hacía absolutamente imposible la inteligencia a quien no tuviese la clave[...].***
>
> ***Muchos juzgaron esta hazaña, y no sin alguna verisimilitud, superior a toda humana industria, y según refiere Jacobo Augusto Thuano, los Españoles dieron algunas quejas en Roma, de que los Franceses usaban de artes diabólicas para penetrar sus secretos. Pero la verdad era, que no había intervenido en este negocio más diablo que un espíritu de rara comprensión, y sutileza, ayudado de una aplicación infatigable; pues se cuenta de este raro hombre, que algunas veces sucedió estarse tres días con sus noches embelesado en sus especulaciones Matemáticas, sin comer, ni dormir, salvo un brevísimo reposo que tomaba, reclinándose sobre el brazo de la silla".-***

El ***espíritu*** *de rara compresión* del que habla el padre Feijoo es François Viéte, matemático francés considerado uno de los precursores del álgebra, que simplemente a base de matemáticas, trabajo y paciencia consiguió quebrantar la "indestructible" cifra general.

1.2.2. Luis Valle de la Cerda

Puesto que los textos materia de estudio son de Luis Valle de la Cerda, vale la pena detenerse un poco en su figura y contexto, antes de analizar los documentos.

El nivel alcanzado por la criptografía de la Casa de Austria en España puede reflejarse en el conjunto de todas las cifras utilizadas desde Felipe II y publicadas en su día por J.P. Devos pero también en los diferentes sistemas particulares empleados por los agentes y espías al servicio de la Monarquía Hispánica que utilizaron en sus correspondencias particulares con los miembros de su red.

De estos sistemas y de la pericia para alcanzar el éxito en la particular dialéctica "encriptación-criptoanálisis", es decir, "cifrado y descifrado" hablaría, como ejemplo válido, el manuscrito nº 994, custodiado en la Biblioteca Nacional de Madrid. En su

seno encontramos, a modo de "méritos y servicios criptográficos", la exposición por parte del consejero don Luis Valle de la Cerda, secretario de la cifra y contador del consejo de Cruzada, con inclusión de varios testimonios originales de cartas descifradas de su mano, ofreciéndonos el retrato de un experto criptoanalista de finales del siglo XVI y comienzos del siglo XVII.

El memorial y cartas descifradas adjuntas nos proporcionan alguna información más detallada sobre la formación y pericia adquirida por dicho secretario. El ejemplo de Valle de la Cerda nos permite detenernos en torno a una figura como esta, la del secretario, centro y objeto de atención de no pocas reflexiones políticas y administrativas durante los siglos XVI y XVII:

> *Luis Valle de la Cerda, que fue secretario del Consejo de su Magestad y su contador en el de la Sancta Cruzada y su secretario de la cifra después de aver continuado en la Universidad de Salamanca por algunos años los estudios y averse graduado en ella el año de 1577, deseando con muy natural inclinación y affecto emplearse en el servicio de su Magestad desde edad de 18 años salió de España y passó a Roma el año de 78 de donde aviéndose enterado con muy particular inteligencia y noticia de las cosas de Italia passó el año de 81 a los estados de Flandes donde estuvo entretenido cerca de la persona del Príncipe de Parma, Governador y Capitán General. Sirvió a su Magestad del Rey don Phelippe segundo en negocios gravissimos y de grande importancia particularmente en secretos y papeles de mucha confianza descifrando sin contracifra cartas y correspondencias de los enemigos y factores d elos rebeldes y herejes y de otros príncipes en lenguas diversas de que se consiguieron grandes emolumentos en negocios de estado y guerra y se sacaron tantas advertencias, avisos y secretos como en la guerra se encubren debajo de tales caracteres y figuras con el discurso y orden siguiente […] Y en los dichos estados de Flandes continuó estos servicios hasta el año de ochenta y nueve descifrando sin contra cifra correspondencias engañosas y de grande daño del Reyno de Inglaterra y descubriendo y sacando a la luz tratos, estratagemas y engaños de enemigos de la Iglesia cathólica, particularmente una carta que se alcanzó a tomar de un ministro de la Reyna de Inglaterra el año de 85, ganado Amberes, en cifra y lengua latina de cuya declaración se entendió el trato que tenían hecho los rebeldes queriendo entregar a Frigilingas, Brilla y otras fuerzas de Olanda y Zelanda, como sucedió un mes después, que puedo ser de grande emolumento de la Iglesia y indecible servicio de su Magestad a tener en aquellos estados suficiente socorro y auxilio para tan grande daño. Con estos y otros muchos servicios no se apartó por espacio de otros cinco años de todas las*

ocasiones y movimientos de guerra no rehusando ni perdonando a muchos riesgos y peligros de la vida por ser su persona tan conocida y buscada de los enemigos que se carteaban con semejantes engaños deseando sumamente quitársela porque no hallasen estorvo sus dañados intentos y designios. Y en esta tan peligrosa ocasión fue captivado y preso por los ingleses y llevado a Vergas estrivando solamente su vida en que no conociesen quién era; pues después de haverse librado por favor de Dios a costa de su propia hazienda daba la Reyna de Inglaterra muchos ducados por su cabeza con grandíssima cólera y despecho por aver sabido que avía estado en su mesmo reyno cautivo. Descifró después en otras ocasiones con semejante utilidad y aprobación como fue una carta de Venecia que le dio en Turín la señora infanta doña Catalina por orden del duque de Saboya quando tenía sitiada Ginebra. (12)

1.3. OBJETIVOS DEL PRESENTE PROYECTO

El objetivo de este proyecto es el análisis de varios textos cifrados de los siglos XVI y XVII y su desciframiento cuando sea posible. Para ello se estudiarán detenidamente ciertos parámetros estadísticos de cada uno de los documentos, como la entropía, el histograma y la autocorrelación. Estos parámetros serán de gran ayuda a la hora de describir la fortaleza de los métodos de cifrado y el tipo de sistema que se ha utilizado. Además en los casos en que el sistema utilizado no sea evidente se realizará un estudio comparativo entre los textos analizados con el fin de alcanzar conclusiones fiables que serán de gran utilidad de cara a futuras líneas de investigación.

En el apartado 3 de la memoria se explica detalladamente la metodología seguida y las herramientas empleadas para conseguir el cumplimiento de los objetivos anteriormente mencionados.

1.4. ORGANIZACIÓN DEL DOCUMENTO

El presente proyecto está dividido en cinco secciones, cuyo contenido se detalla a continuación.

- **Introducción**: ofrece una visión general de la criptografía, desde su origen conocido hasta finales del siglo XVII. Incluye cuatro subsecciones:

- En la primera subsección se realiza un recorrido histórico a través del periodo de tiempo mencionado.
- La segunda subsección se centra en la criptografía en España en los siglos XVI y XVII (siglos de los que datan los textos analizados) y además se realiza también un pequeño estudio de la figura de Luis Valle de la Cerda, por la importancia que tiene en la criptografía de la época y, más concretamente, en los documentos que son objeto de estudio de este proyecto.
- La tercera subsección indica brevemente los objetivos de este proyecto.
- La cuarta subsección explica la forma en que se ha organizado esta memoria.

- **Estado de la cuestión**: en esta sección se detalla brevemente la situación de los textos cifrados de esta época, dónde se conservan los manuscritos de que se dispone, y además se citan algunos de los investigadores de criptografía más importantes en la actualidad. Se nombran además diversas publicaciones y proyectos de interés y sitios web de importancia dedicados exclusivamente a esta disciplina.

- **Metodología seguida y herramientas empleadas**: en esta tercera sección se divide a su vez en tres apartados:
  - El primero de ellos presenta los textos que van a ser analizados así como su contexto histórico.
  - El segundo apartado presenta la herramienta a través de la cual se va a realizar el análisis.
  - El tercer apartado define intuitiva y formalmente los parámetros que se van a calcular de cada uno de los documentos, así como el significado de los distintos valores que se puede obtener, aplicados al análisis de estos documentos.

- **Análisis y Resultados obtenidos**: esta sección muestra los resultados obtenidos para cada uno de los textos analizados y, basándose en dichos resultados, plantea diversas hipótesis, además de apuntar las conclusiones que ese detallarán en la siguiente sección. Consta de cuatro subsecciones, una por cada texto analizado, y otra en la que se realiza un estudio comparativo que sirve como base a las hipótesis mencionadas.

- **Conclusiones y Líneas futuras de investigación**: esta última sección resume lo obtenido en la sección anterior y muestra las conclusiones que se han alcanzado. Además plantea, a la vista de los resultados obtenidos, posibles futuras líneas de investigación interesantes para las que los resultados de esta memoria serían de gran utilidad.

Además de estos cinco grandes apartados, esta memoria consta también de un resumen de la misma que se encuentra antes de la sección de *Introducción*. Tras la sección de *Conclusiones y Líneas futuras de investigación* se encuentra un apartado que recoge la bibliografía y las referencias utilizadas para el desarrollo del proyecto, y un apartado de *Anexos*, donde se incluyen los documentos originales sobre los que se ha trabajado, un presupuesto detallado y otros documentos de interés que han sido citados a lo largo de la memoria, como la Cifra General de Felipe II, una Cifra Particular y un nomenclátor.

CAPÍTULO 2

ESTADO DE LA CUESTIÓN

2. ESTADO DE LA CUESTIÓN

Durante todo el período de la España de los Austrias, y durante el siglo anterior, nuestros gobernantes hicieron amplio uso de la criptografía. Existen publicaciones específicas donde se incluyen docenas de cifras y claves diversas. En el Archivo General de Simancas la gran colección de legajos de la Secretaría de Estado incluye un "legajo cero" titulado sencillamente "cifras", que contiene las cifras oficiales de casi dos siglos de gobernantes españoles. Algunas de esas cifras están perfectamente descritas por año y usuarios, en tanto que otras solamente llevan indicaciones vagas del tipo "es letra del siglo XVI" o "del tiempo de la ocupación española de Portugal", y de otras solamente se conoce el nombre o el seudónimo del usuario, o ni siquiera eso. Solamente algunas de esas cifras han sido publicadas o estudiadas. (13)

La época de más interés en la escritura cifrada española probablemente sea la del reinado de Felipe II. En sus comienzos, el 24 de mayo de 1556, escribió desde Bruselas una carta a su tío el Emperador Fernando I en la que comunicaba estar resuelto a variar la cifra que usaba Carlos V, "no sólo por ser antigua y haber muerto muchos y otros mudado de destino de los que estaban en el secreto, sino por estar también harto divulgada y no convenir, por esta razón, al buen éxito de los negocios". (14)

El Archivo General de Simancas, iniciado por Carlos V y finalizado por su hijo Felipe II, guarda toda la documentación producida por los organismos de gobierno de la monarquía hispánica desde la época de los Reyes Católicos (1475) hasta la entrada del Régimen Liberal (1834). Constituye, pues, el fondo documental más homogéneo y completo de nuestra memoria histórica de los siglos XVI al XVIII (15). Del reinado de Felipe II se conservan en el archivo general de Simancas las cifras generales para los años 1562, 1567, 1568, 1571, 1572, 1574, 1575 y 1582 y las particulares para con el duque de Alba y con los embajadores don Francés de Alba y don Guenán de Espés. Otras, sin fecha, se atribuyen a la misma época.

La dificultad principal con la que los investigadores que manejan papeles de Estado tropiezan continuamente, es la correspondencia cifrada tan abundante en esta sección. Algunas cifras, sobre todo las generales de Felipe II, de las que ya se ha

hablado, contienen cientos de nombres, lo que dificulta que alguien, por muy hábil que sea, pueda descubrir la correspondencia de cada uno de esos signos. A pesar de los grandes trabajos e investigaciones llevados a cabo en esta materia, queda aún bastante trabajo por hacer.

Se conocen muchas claves de las utilizadas en la época pero aún hoy es válido el juicio de Mariano Alcocer Martínez, afirmando que "en nuestros archivos existen todavía muchísimos documentos sin descifrar". (14)

Por otra parte, en este *estado de la cuestión* se nombran algunos de los investigadores y de las publicaciones actuales altamente relevantes en la situación actual de la criptografía. La bibliografía de este proyecto incluye bastantes obras de estos investigadores.

Hoy en día la información puede que sea uno de los bienes más preciados, o la desinformación una de las peores armas con las que atacar a alguien. En la sociedad actual se hace muy necesaria la seguridad en las comunicaciones, especialmente en Internet, ya que este método de comunicación es cada vez más utilizado por todo tipo de usuarios. Por todo ello cabe pensar que la criptografía será uno de los claros factores a tener muy en cuenta en el futuro inmediato de la informática, sobre todo a la velocidad que se implementan nuevas tecnologías, las cuales permiten el envío de información que puede comprometer mucho a los interlocutores en caso de ser interceptada por otras personas. Lo cierto es que se trata de un mundo fascinante y que tiene muchas posibilidades de investigación. Son muchos los expertos e investigadores unidos a las redes de investigadores y colegios invisibles (grupos de científicos interesados por un mismo tema que intercambian trabajos e información sobre dicho tema) los que en la actualidad están trabajando y desarrollando nuevas líneas de investigación dentro del campo de la criptografía. Dentro de esta gran lista cabe destacar especialmente:

David Kahn, historiador estadounidense, periodista y escritor. Se ha dedicado casi exclusivamente a escribir sobre la historia de la criptografía, inteligencia militar y diversos temas relacionados. Fue nombrado doctor por la Universidad de Oxford en

1974 en el área de Historia Moderna de Alemania, bajo la supervisión del profesor de historia moderna Hugh Trevor-Roper.

El primer libro de Kahn fue *The Codebreakers* publicado en 1967, considerado una obra maestra y libro de referencia en temas de historia de la criptografía. Supuso una novedad en la época de su publicación. Una de las ediciones inglesas de 1996 tiene un capítulo adicional con una recolección de los eventos acaecidos en criptología desde la aparición de la primera edición, tal como el advenimiento de sistemas criptográficos populares tales como el PGP. La novela *The Codebreakers* fue finalista para el premio Pulitzer en el año 1968 dentro de la categoría de no ficción.

Son de gran importancia todas las publicaciones realizadas por los colegios invisibles; especialmente, y debido a su gran interés, cabe señalar ***Cryptologica***, revista trimestral americana que publica todos los aspectos relacionados con la criptografía. El primer volumen fue publicado en enero de 1977. Constituye una publicación única para los estudiantes interesados en todos y cada uno de los temas relacionados con criptología. Los artículos que en ella se incluyen han abierto muchos nuevos caminos en la historia de la inteligencia. Se contó por primera vez cómo una agencia especial preparó la información de descifrado para el presidente Roosevelt, se han descrito las cifras de Lewis Carroll, revelado los detalles de la agencia de intervención de las conexiones telefónicas de Hermann Goering y publicado la metodología de algunos descifradores americanos de la segunda Guerra Mundial. Además se expuso cómo los descifradores de código americanos afectaron la estructura de la organización de Naciones Unidas. También ha realizado traducciones relevantes: por un lado, las partes árabes de los primeros textos líderes mundiales sobre criptoanálisis y, por otro lado, del alemán un estudio de criptoanálisis nazi. Publicó también un artículo basado en un área hasta ese momento desconocida: el Frente occidental alemán de descifrado en la primera guerra mundial. Publica también artículos técnicos de análisis del criptosistema generado por máquinas de cifra, incluyendo la Enigma, además de relatar la solución de criptogramas históricos. Explicaron la base lingüística de la lengua navaja usada por cifradores en el océano Pacífico y comunicaciones digitales que pueden ocultar ilustraciones o imprimir con filigrana lo que autentica la fuente. Un artículo demostró la insuficiencia de cifras basadas en la música, entre otras cosas.

Otras revistas de interés acerca de criptografía son *Intelligence and National Security* estudiando con profundidad los ataques biológicos y no gubernamental, las principales dificultades encontradas en cuanto a seguridad por el departamento de inteligencia, analistas de inteligencia y fabricantes de política, y los beneficios y peligros de la tensión existente en las relaciones entre el servicio de inteligencia y el público en general, además de otros temas de gran interés. Existen además otras muy similares tales como *International Journal of Intelligence and Counterintelligence* y *Studies in Intelligence.*

Es muy amplio y extenso lo referente a criptografía aplicada a la historia y tecnología militar. Existen muchos artículos en revistas que nos pueden dar una idea de cuáles son las líneas de investigación y proyectos que más interesan a los militares en cuanto a los temas de seguridad de la información y criptografía aplicada.

De los expertos e investigadores que en la actualidad están trabajando y desarrollando nuevas líneas de investigación dentro del campo de la criptografía, conviene destacar a Juan Carlos Galende Díaz y a Jorge Ramió Aguirre.

Juan Carlos Galende Díaz, doctor en historia por la universidad Complutense de Madrid y profesor titular del departamento de Ciencias y Técnicas Historiográficas de la Facultad de Geografía e Historia, del que es actualmente su director, integrante de diferentes equipos de investigación nacional e internacional. Ha realizado diversos escritos como: *Catálogo concordado de los repertorios bibliográficos de Hernando Colón*, *Diccionario Histórico de la Antroponimia Románica*, *Documentación epigráfica y paleográfica de interés científico-cultural e Histórico-social para la Comunidad de Madrid*, *La organización del espacio en la Corona de Castilla (1212-1369)* etc. y es además autor de diversas monografías (*Criptografía. Historia de la escritura cifrada*, *Diccionario general de abreviaturas españolas*, La *crisis del siglo XVIII y la Inquisición española*, *El caso de La Inquisición toledana* (1700-1820), *Antroponimia madrileña del siglo XVII*, *Historia y Documentación*...) y artículos de carácter paleográfico-diplomático, entre los que destacan los temas criptográficos, cronológicos, archivísticos, bibliotecarios, etc.

Jorge Ramió Aguirre, coordinador de la Red Telemática Iberoamericana de Criptografía y Seguridad de la Información (CriptoRed). Es también profesor del

Departamento de Lenguajes, Proyectos y Sistemas Informáticos de la Universidad Politécnica de Madrid. El fin de Criptored era que algún día el conjunto de países Iberoamericanos (Latinoamérica, España y Portugal) estuviesen integrados en ella con representantes de sus universidades, centros de investigación, instituciones y empresas. Ello sería una prueba de que ese objetivo de integración que se propugna a través de Internet por medio de las denominadas Comunidades Virtuales se ha cumplido, como así ha sido en estos más de 10 años de vida de una de las redes temáticas decanas en el mundo. Para ello se ha contado con la especial colaboración de la comunidad científica de estos países.

Se indican estos dos investigadores tan solo a modo ilustrativo, aunque, evidentemente, existe un gran número de investigadores que están llevando a cabo diversas líneas de temas relacionados con la criptografía tanto internacional como nacional. (16)

Se cita al investigador Jorge Ramió también por ser el creador de Intypedia (InformationSecurity Encyclopedia). Se trata de un proyecto de la red temática Criptored de reciente creación que, mediante un conjunto de lecciones diseñadas por destacados expertos invitados, recorre los diversos ámbitos de la Seguridad de la Información, como los fundamentos de la historia de la criptografía, y temas más actuales como la seguridad en redes de Internet, autenticación y firma digital, etc. En esta primera fase participan: Arturo Ribagorda Garnacho de la Universidad Carlos III de Madrid, Fausto Montoya Vitini del Consejo Superior de Investigaciones Científicas de Madrid, Gonzalo Álvarez Marañón también del Consejo Superior de Investigaciones Científicas de Madrid y Justo Carracedo Gallardo de la Universidad Politécnica de Madrid. (17)

CAPÍTULO 3

METODOLOGÍA SEGUIDA Y HERRAMIENTAS EMPLEADAS

3. METODOLOGÍA SEGUIDA Y HERRAMIENTAS EMPLEADAS

El objetivo de este proyecto es el análisis de varios textos cifrados de los siglos XVI y XVII y el estudio de su fortaleza a través del cálculo de diversos parámetros, como la entropía y la autocorrelación.

3.1. TEXTOS ANALIZADOS

Utilizaremos la herramienta Cryptool para el estudio de dos documentos principales que se pueden consultar en el anexo de esta memoria:

1. Cifra de los secretos de las minas de la India hecho por Luis Valle de la Cerda después de declarada. (Siglo XVII).
2. Cifra que Geronimo Sertori Milanés ofreció a su majestad por suya, y el consejo de estado la cometió para que la viese Luis valle de la cerda, el cual mostró al dicho Sertori un papel en que estaba la misma declarada por el rey don Felipe segundo. (Siglo XVI)

Los funcionarios reales en las Indias y los conquistadores, cada vez que se tenía conocimiento de un descubrimiento minero de importancia o que desde los puertos americanos se hacía una remisión de oro y plata que afectase a la Real Hacienda, de inmediato transmitían la información a la Casa de la Contratación, en cuanto organismo regulador de las colonias, y a la Corona, siendo numerosos los escritos conservados de este tenor en los fondos del AGI (Archivo General de Indias) dirigidos personalmente a los Reyes, a la reina Juana, al emperador, a la emperatriz o al príncipe Felipe, dando cuenta de las remisiones hechas. Menudean los escritos de Pedrarias, Vázquez de Carvajal, Espinosa, Pizarro, Cortés, Gama Albornoz, Valdivia y un largo etcétera que, junto a la jerarquía eclesiástica colonial o clero regular y secular mostraron el prurito de mantener informada a la Corona por razones de sus particulares conveniencias y como medio de atraerse el favor regio en sus aspiraciones de promoción social y política en las colonias; los funcionarios reales de Cuba, Cartagena, Santa Fe, Nicaragua, Perú, México, Panamá, San Juan, etc., hacían otro tanto con información directa a los reyes o a través de sus secretarios, como Francisco de los Cobos, por idénticas razones, acordes con un proceder habitual de la burocracia al servicio de las Monarquías nacionales.

El 1 de junio de 1574 se ordena que haya lista y relación de las minas existentes en cada distrito de Indias para ser enviada al Consejo; una información que se codificará a efectos de salvaguarda y uso de régimen interno de la administración colonial: en 1509, el rey da órdenes al tesorero en indias, Pasamonte, para que este, cuando escriba a Lope Conchillos dando noticias de las riquezas americanas, mantenga el secreto utilizando "la cifra que de acá llevasteis concertada con el dicho secretario"; lenguaje cifrado que se formaliza como medio habitual de comunicación en la administración colonial en cuanto tocase a la riqueza del oro y la plata, como aparece en el texto de Valle de la Cerda de 1605 sobre la cifra de *los secretos de las minas de Indias*. (18)

Según Guillermo Lohmann, *ni la contracifra matriz ni el alfabeto que Valle de la Cerda logró reconstituir, expresivo de los espectaculares signos convencionales ideados por Orozco y Gamarra, acompañan hoy al documento original. Manos inescrupulosas los han sustraído*. (19)

En cuanto al segundo documento analizado, apenas se dispone de datos sobre su contexto, tan solo la parte de texto que aparece al comienzo del documento cifrado.

3.2. HERRAMIENTA UTILIZADA

La herramienta utilizada para todos los documentos estudiados ha sido Cryptool; se trata de una aplicación de aprendizaje electrónico gratuita para Windows. Puede utilizarse para aplicar y analizar algoritmos criptográficos. La versión actual de CrypTool se utiliza en todo el mundo. Soporta tanto los métodos actuales de enseñanza en escuelas y universidades como también la concienciación de los empleados. Es el programa de aprendizaje electrónico de uso más extendido en el mundo en el área de la criptología.

3.2.1. Introducción

CrypTool es un software libre que ilustra conceptos criptográficos. Es el programa de aprendizaje electrónico de uso más extendido en el mundo en el área de la criptología. CrypTool se utiliza en universidades, en institutos educativos así como también en formación profesional en las empresas. Es un esfuerzo realizado por más de

40 colaboradores alrededor de todo el mundo. Es una herramienta que se lleva a cabo en un Proyecto de código abierto. Su papel consiste en hacer que los usuarios tomen conciencia de las amenazas de seguridad de la red y explicarles algunos de los conceptos subyacentes. Se ha diseñado tanto como una herramienta de aprendizaje electrónico (e-learning) como un programa para usarlo de forma productiva.

La versión actual ofrece, entre otras cosas, lo siguiente:

- Numerosos algoritmos criptográficos, clásicos y modernos (cifrado y descifrado, generación de clave, contraseñas seguras, autentificación, protocolos seguros, ...)
- Visualización de varios métodos (p.ej. César, Enigma, RSA, Diffie-Hellman, firmas digitales, AES)
- Criptoanálisis de ciertos algoritmos (p.ej. Vigenère, RSA, AES)
- Métodos de medida criptoanalítica (p.ej. entropía, n-grams, autocorrelación)
- Métodos auxiliares (p.ej. tests de primalidad, factorización, codificación en base64)
- Tutorial sobre teoría de números.
- Ayuda detallada on-line.
- Script con más información sobre criptografía.

Desde su uso original para la formación en seguridad de una compañía, CrypTool ha evolucionado en un destacado proyecto de código abierto para temas relacionados con la criptografía.

Desde la primavera de 2008, está funcionando dentro del proyecto CrypTool el Cripto Portal para profesores. Por ahora el portal sólo está disponible en alemán y se espera que actúe como una plataforma para que los profesores puedan compartir material para la enseñanza de la criptografía y temas relacionados. (20)

3.3. PARÁMETROS ESTUDIADOS

Se analizará cada uno de los sistemas a través del estudio de su entropía, análisis de frecuencias y autocorrelación para analizar su robustez criptográfica. Definiremos estos términos desde un punto de vista criptográfico:

3.3.1. Entropía

De forma intuitiva la entropía puede ser entendida como la cantidad de información promedio que contienen los símbolos usados. Los símbolos con menor probabilidad son los que aportan mayor información; por ejemplo, si se considera como sistema de símbolos a las palabras en un texto, palabras frecuentes como "que", "el", "a" aportan poca información, mientras que palabras menos frecuentes como "corren", "niño", "perro" aportan más información (si de un texto dado borramos un "que", seguramente no afectará a la comprensión y se sobreentenderá, no siendo así si borramos la palabra "niño" del mismo texto original). Cuando todos los símbolos son igualmente probables (distribución de probabilidad plana), todos aportan información relevante y la entropía es máxima.

Para una definición formal ha de plantearse antes la cantidad de información que aporta un determinado valor (símbolo), X, definida como:

$$I(x_i) = \log_2 \frac{1}{p(x_i)} = -\log_2 p(x_i)$$

La entropía determina el límite máximo al que se puede comprimir un mensaje usando un enfoque símbolo a símbolo sin ninguna pérdida de información (demostrado analíticamente por Shannon), el límite de compresión (en bits) es igual a la entropía multiplicada por el largo del mensaje. También es una medida de la información promedio contenida en cada símbolo del mensaje. Su cálculo se realiza a partir de su distribución de probabilidad p(x) mediante la siguiente fórmula:

$$\begin{aligned} H(X) = \mathrm{E}(I(X)) &= \sum_{i=1}^{n} p(x_i) \log_a \left(\frac{1}{p(x_i)}\right) \\ &= -\sum_{i=1}^{n} p(x_i) \log_a p(x_i) \end{aligned}$$

Valores extremos de la entropía

En documentos formados únicamente por letras mayúsculas la entropía estará entre 0bit/símbolo (un documento que consiste en un solo símbolo) y log(26) bit/símbolo = 4.700440 bit/símbolo (un documento en que los 26 símbolos aparecen con la misma frecuencia).En documentos que pueden contener cualquier símbolo del conjunto de caracteres (de 0 a 255) la entropía variará entre 0 bit/símbolo (un documento que consiste en un solo símbolo) y log (256) bits/símbolo = 8 bits/símbolo (un documento en el que los 256 símbolos aparecen con la misma frecuencia).

Para nuestro estudio, cuanto mayor sea el valor de la entropía, más robusto será el sistema de cifrado. Sin embargo la entropía no es suficiente para determinar la fortaleza del sistema, por lo que se estudiarán otros parámetros adicionales.

3.3.2. Análisis de frecuencias

Se realizará a través del histograma. La situación ideal es que todos los caracteres aparezcan con la misma frecuencia, siendo así más complicado el descifrado del documento. Por el contrario, si el histograma es desigual y las frecuencias presentan grandes variaciones entre símbolos, el cifrado será débil y fácilmente recuperado el documento original a través de un estudio de frecuencias del idioma en que se escribió. Por ejemplo, si nos consta que el idioma es el español, el símbolo con la mayor frecuencia probablemente represente la letra "E". (21)

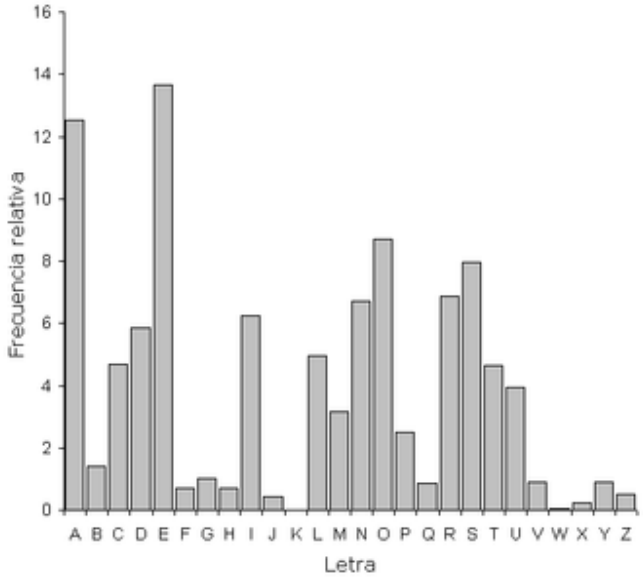


Figura 7. Frecuencia de letras en la lengua española (21)

Para obtener información más directa de cada uno de las frecuencias, se estudiará también el N-grama, que proporciona una tabla indicando la frecuencia de todos o parte de los caracteres del histograma. Esta herramienta también permite obtener las frecuencias de los bigramas, trigramas, etc., datos que pueden ser de gran utilidad en ciertos casos.

3.3.3. Autocorrelación

La función de autocorrelación c(t) calcula la similitud entre las secuencias (s[i])=s[1] s[2]... y (s[i+t])=s[t] s[t+1]...., que es la misma secuencia desplazada "t" unidades.
Si se analiza una secuencia de longitud n, se definen los siguientes parámetros:

- A(t) := número de elementos de las secuencias (s[i]) y (s[i+t]), dentro del segmento considerado, que coinciden.
- D(t) := número de elementos de las secuencias (s[i]) y (s[i+t]), dentro del segmento considerado, que no coinciden.
- La función de autocorrelación C(t) = (A(t)-D(t)) / n.

En el caso de secuencias finitas, se desplazan "t" posiciones, de manera que la secuencia (s[i+t]) solo conste de "n-t" elementos (donde "n" es la longitud de la secuencia (s[i]). Para calcular la autocorrelación, ahora solo consideramos las secuencias s[1] s[2]... s[n-t+1] y s[t] s[t+1]... s[n] y calculamos su correlación.

La función de autocorrelación se usa, entre otras cosas, para averiguar la longitud de la clave de un documento cifrado mediante métodos de encriptado clásico, siendo la longitud máxima de dicha clave de 1024 caracteres.

CAPÍTULO 4

ANÁLISIS Y RESULTADOS OBTENIDOS

4. ANÁLISIS Y RESULTADOS OBTENIDOS

En este apartado se realizará el estudio estadístico de tres textos. El objetivo de este estudio no es descifrar los textos sino realizar un análisis de los métodos utilizados para su cifrado, así como de su fortaleza. Del documento de las minas se disponía de la contracifra correspondiente, por lo que además del análisis del sistema utilizado, se ha descifrado parte del documento. Además se incluye un tercer texto de la época sin cifrar, y de temática y registro similar al previamente descifrado para establecer una comparativa entre los tres documentos. Este estudio comparativo será de gran utilidad a la hora de sacar conclusiones sobre ciertos aspectos de los sistemas utilizados.

4.1. DOCUMENTO 1: TEXTO SERTORI (SIGLO XVI)

El primer paso para el estudio del documento (consúltese en el anexo V) es transcribirlo en caracteres que nos sean conocidos. En este caso el documento cuenta con 27 caracteres diferentes; utilizaremos para representarlos tanto letras del alfabeto ordinario como números. El alfabeto resultante con el que haremos la transcripción es:
ABCDEFGIJKLMNOPRSUXY2345890

La correspondencia entre caracteres se puede ver en la siguiente tabla:

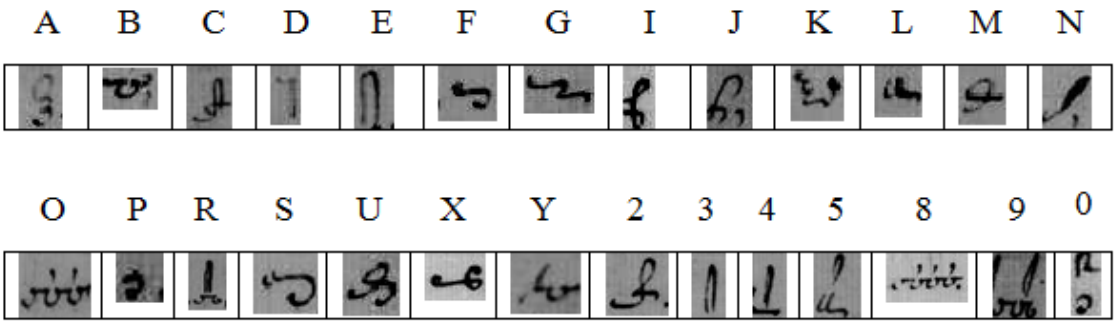


Figura 8. Correspondencia de caracteres texto Sertori

La transcripción del texto con los nuevos caracteres es la siguiente:

AYCLPDEAFGRF3RNFCSPFJPKEPOSLMEJBBNGDKNMMPPJSFPFB3SGDPKJRB3MF39ANLP
ONLPYRSRPFPFNGD2CPSALAUB3OB3KJB3NFNBECPNGANLB3PMNNBRSENF3PNBSJRNG
EDLPKEDGK20KCN4CF3JEESNLODPUPNROZNGF3JNB3BSJZDK5ANPSNPNN6GF3JNRSF3J
JNB3BKIADOCKN4F3SJB3B3SLJNBNF3GNPJPNBF3RNA3DSNANNBDNANBNB3RNSK8NC
PF3LEADUF3B3UNB3FASKSNLD24EAKGAF3NNBSJF3NP555DF3GCPB3JB3AMMPB3KRSL
PNBRSF3NPF3G5ESDF32NBCSKAF3LUKPB3NBOGRKJB3UDF3CP8KNDUPNBNRF3DAGAG
B32B3NBSPR2ANPF3DKNS3RNDFNBKD8F3NFB3UR2PF3GSFFNDP8PJJNBSB3NNBSP23Z
F3NDNS3KL3JF3B3NPNBNSGS3RPDKNAF3KL3PB3KNEDEPNF3XSRF3LPNPLXPF3GB3LDN
BFF3NPL8LNXLSKPB35DF3ZSNR2GALZAF3LKPNNBEPJRPNBKS3EBBBB3YLNGLPJMPMSN
BAPANLRB3ENKPRENANBNBYANB3B3P2DLNBPARPEJB35KF35DANBB32AJKPEPMC8SE
B3SLDF3GAPRYNPJNBDPRF3PNLBBNGEKPNKB3B3RNSLBBB3F3RYNAARPNBNEGKB3NSL
3DRF3XB3PANCPYNGJNBENL

El texto con este formato será el que se introduzca en Cryptool para el estudio de su entropía, análisis de frecuencias y autocorrelación.

- **Entropía**

  La entropía que nos proporciona la herramienta es de 4.09, siendo la entropía máxima posible de 4.75, además aparecen en el documento todos los caracteres del alfabeto con el que se trabaja, resultado por otra parte lógico puesto que hemos sido nosotros los que hemos creado dicho alfabeto en función de la versión cifrada. El valor de la entropía indica que se trata de un sistema de robustez bastante mejorable.

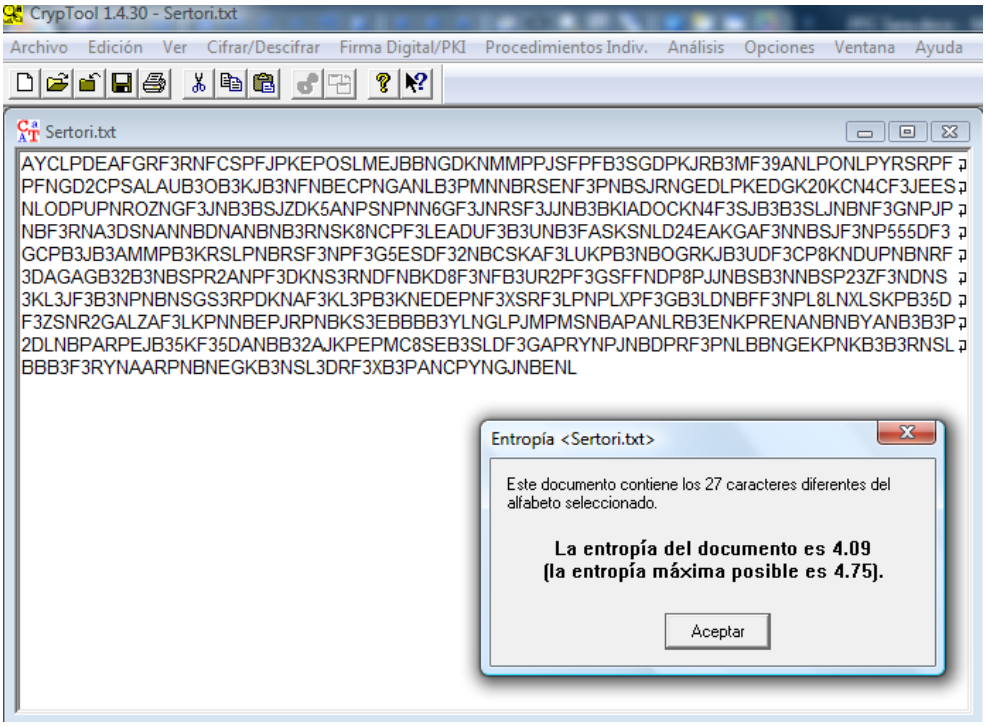


Figura 9. Entropía Sertori

- **Análisis de frecuencias**

El análisis de frecuencias se realizará a través del estudio del histograma y el N-grama, que proporciona una lista de los caracteres ordenados de más a menos frecuente, indicando su frecuencia en porcentaje y en número de apariciones.

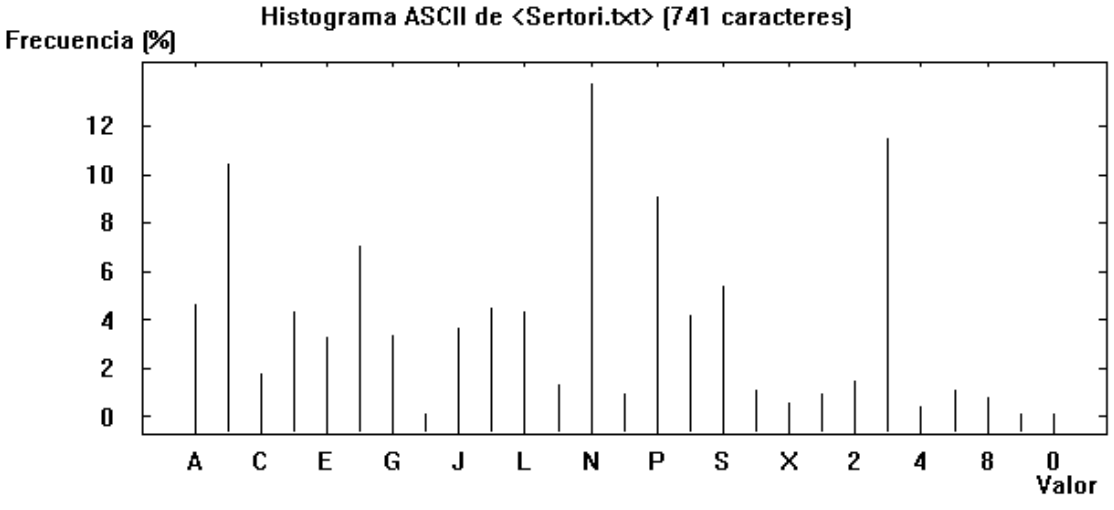


Figura 10. Histograma Sertori

Histograma Análisis de <Sertori.txt>. Tamaño del archivo 749 bytes.
Ordenados descendentemente por frecuencia.

Nº	Subcadena	Frequencia (en %)	Frecuencia
1	N	13.7652	102
2	3	11.4710	85
3	B	10.3914	77
4	P	9.0418	67
5	F	7.0175	52
6	S	5.3981	40
7	A	4.5884	34
8	K	4.4534	33
9	D	4.3185	32
10	L	4.3185	32
11	R	4.1835	31
12	J	3.6437	27
13	G	3.3738	25
14	E	3.2389	24
15	C	1.7544	13
16	2	1.4845	11
17	M	1.3495	10
18	5	1.0796	8
19	U	1.0796	8
20	O	0.9447	7
21	Y	0.9447	7
22	8	0.8097	6
23	X	0.5398	4
24	4	0.4049	3
25	0	0.1350	1
26	9	0.1350	1

Figura 11. N-grama Sertori

Al estudiar tanto el histograma como el N-grama se observa bastante diferencia en la frecuencia de aparición de los caracteres. Como se ha mencionado anteriormente, la situación ideal sería que todos los símbolos presentaran la misma o muy similar frecuencia. En este caso las frecuencias varían bastante de un caracter a otro por lo que se puede concluir que, suponiendo que se tratase de un sistema de sustitución monoalfabética, la robustez del sistema no es demasiado buena.

- **Autocorrelación**

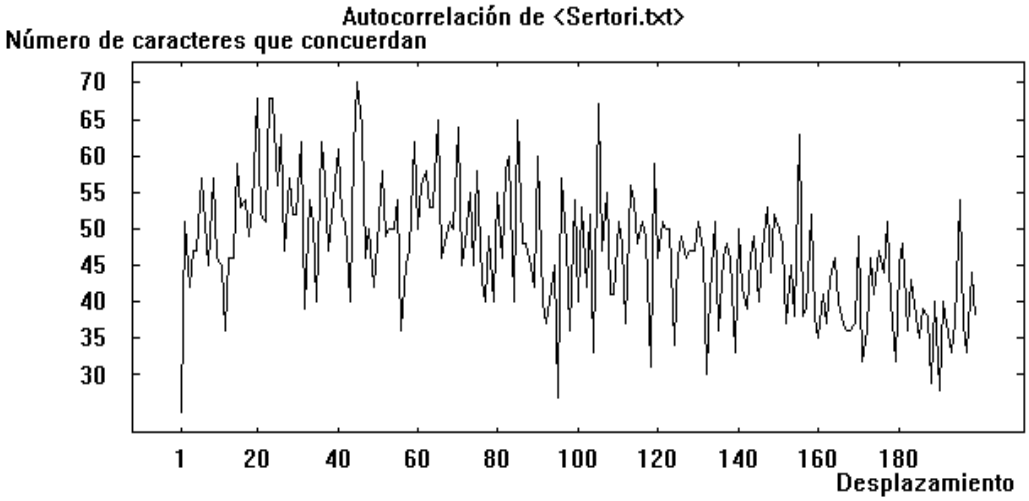


Figura 12. Autocorrelación Sertori

Como se ha mencionado en el apartado teórico, la autocorrelación es útil para determinar la longitud de la clave utilizada en el sistema de cifrado. Se volverá a analizar este parámetro cuando se planteen las conclusiones de los distintos sistemas.

4.2. DOCUMENTO 2: TEXTO MINAS (SIGLO XVII)

Este documento, que se puede consultar en el anexo VI de esta memoria, cuenta con 28 caracteres diferentes, representados por los siguientes caracteres:

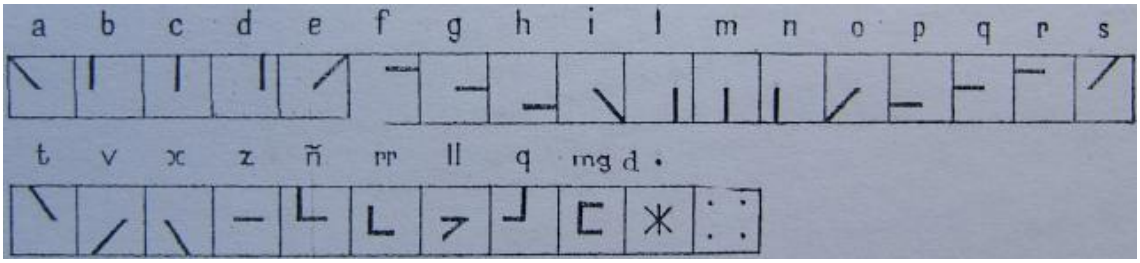


Figura 13. Contracifra texto minas

Hemos descifrado dos de las treinta páginas de que consta el documento, puesto que constituyen un texto de longitud suficiente para realizar el estudio.

El texto descifrado es el siguiente:

en el nombre de dios todopoderoso padre i hixo i espirito santo tres personas i vn solo dios verdadero comiencan los secretos de sacar la maior parte del acogve q se pierde en los rrelaves con la plata q tienen i tanbien de las lamas i de rremoler los rrelaves para volver a sacar plata dellos encorporandolas de nvevo con acogve los qvales secretos a de tratar por mi xvan francisco de rrojas algoacil maior de esta rreal avdiencia de santo domingo el capitán alonso moñon de carvaxal q va a negocios svios a la corte de el rrei nvestro señor en mi nombre para avmento del patrimonio rreal en rracon de lo qval tenemos fecha escritora i lo q aqvi esta escrito tanbien a de tener i tiene foerca de escritora poblica i por tal la otorgamos nos sosodichos fvndamentos q tienen los secretos ariba dichos son dos i anbos se fondan en q sv mg conpre por el preciado monior di mario todos los rrelaves i tanbien las lamas si foere posible q salen de los metales de acogve q se benefician en las minas rricas de potosi i otras del piro i nveva españa por los precios q conpran estas cosas los q volviendo a lavar los rrelaves i q mando sas lamas sacan acogve i plata dellos con aprovechamiento svio los reales precios son diversos conforme al acogve i plata q se poede i soele sacar nellos.

Se puede apreciar la ortografía típica de los siglos XVI y XVII, con características como la doble "r" a principio de palabra, "x" en lugar de "j", "v" en lugar de "u", "c" en lugar de "z", y cierta terminología específica de la minería como relave, lama, azogue, etc.

Tres de los símbolos del documento representan caracteres dobles; para analizar el texto con Cryptool sustituiremos estos caracteres por otros simples que no hayan sido aún utilizados, de la siguiente forma:

 , que representa "rr" en la contacifra, será insertado en Cryptool como "k"

 , que representa "ll" en la contacifra, será insertado en Cryptool como "y"

 , que representa "mg" (magestad) en la contacifra, será insertado en Cryptool como "u".

Además uno de los símbolos representa un signo de puntuación, que también será sustituido por un carácter simple para facilitar la creación de un alfabeto para ser estudiado con Cryptool:

 , que representa "·" en la contracifra, será insertado en Cryptool como "w".

Además la letra "ñ" no es admitida por la herramienta, por lo que también habrá de ser sustituido antes del análisis:

 , que representa "ñ" en la contracifra, será insertado en Cryptool como "j".

Por tanto, el alfabeto utilizado para el análisis del texto es el siguiente:

ABCDEFGHILMNOPQRSTVXZJKUYW

De esta manera, el texto modificado que se analizará con la herramienta Cryptool es el siguiente:

En el nombre de dios todopoderoso padre i hixo i espirito santo tres personas i vn solo dios verdadero comiencan los secretos de sacar la maior parte del acogve q se pierde en los Kelaves con la plata q tienen i tanbien de las lamas i de Kemoler los Kelaves para volver a sacar plata deYos encorporandolas de nvevo con acogve los qvales secretos a de tratar por mi xvan francisco de Kojas algoacil maior de esta Keal avdiencia de santo domingo el capitán Alonso moñon de carvaxal q va a negocios svios a la corte de el Kei nvestro señor en mi nombre para avmento del patrimonio Keal en Kacon de lo qval tenemos fecha escritora i lo q aqvi esta escrito tanbien a de tener i tiene foerca de escritora poblica i por tal la otorgamos nos sosodichos fondamentos q tienen los secretos ariba dichos son dos i anbos se fondan en q sv U conpre por el preciado monior di mario todos los Kelaves i tanbien las lamas si foere posible q salen de los metales de acogve q se benefician en las minas Kicas de potosí i otras del piro i nveva España por los precios q conpran estas cosas los q volviendo a lavar los Kelaves i q mando sas lamas sacan acogve i plata dellos con aprovechamiento svio los reales precios son diversos conforme al acogve i plata q se poede i soele sacar neYos.

- **Entropía**

  La entropía que nos proporciona la herramienta es de 3.92, siendo la entropía máxima posible de 4.70. En esta parte del documento aparecen 24 de los 26 caracteres del alfabeto con el que se trabaja. El valor de la entropía de nuevo indica una robustez mejorable, resultado bastante lógico, puesto que se trata prácticamente de un sistema de sustitución monoalfabética, siendo la "q" el único carácter que cuenta con dos codificaciones, y con tan solo una sustitución de una palabra completa (magestad).

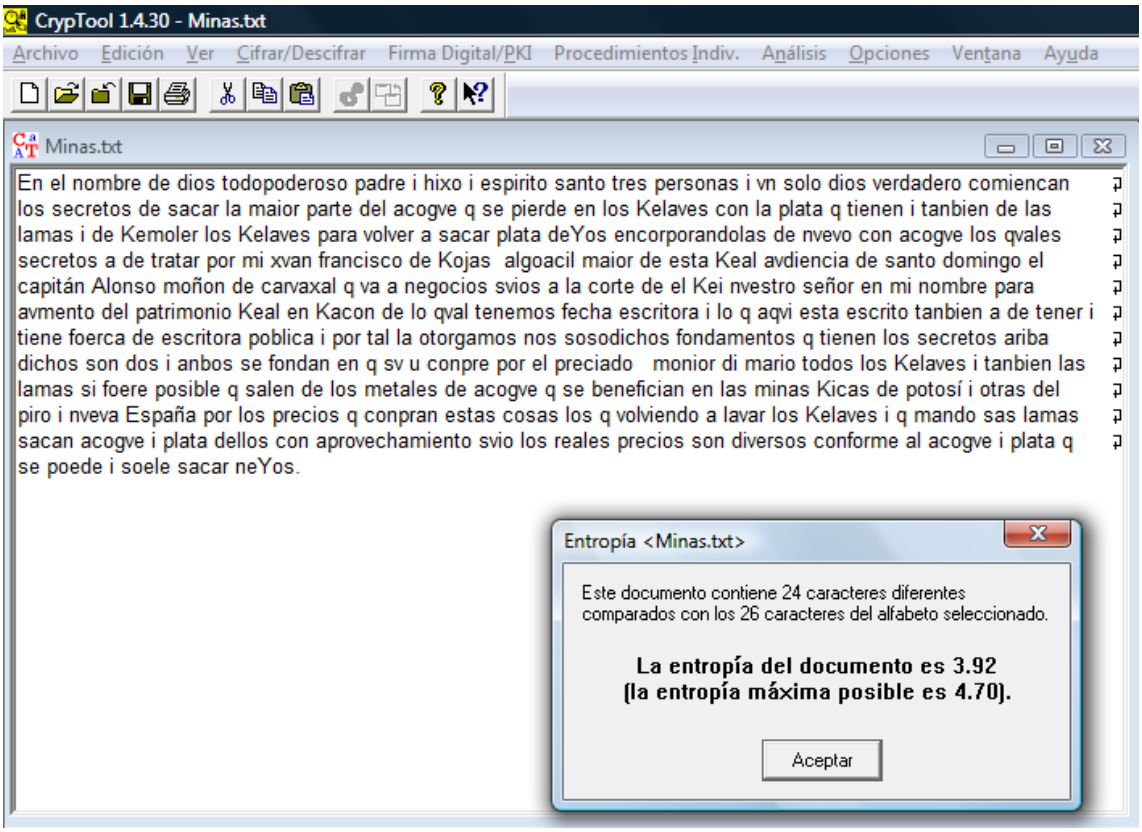


Figura 14. Entropía Minas

- **Análisis de frecuencias**

Como en el texto de Sertori, el análisis de frecuencias se realizará a través del estudio del histograma y el N-grama, que proporciona una lista de los caracteres ordenados de más a menos frecuente, indicando su frecuencia en porcentaje y en número de apariciones.

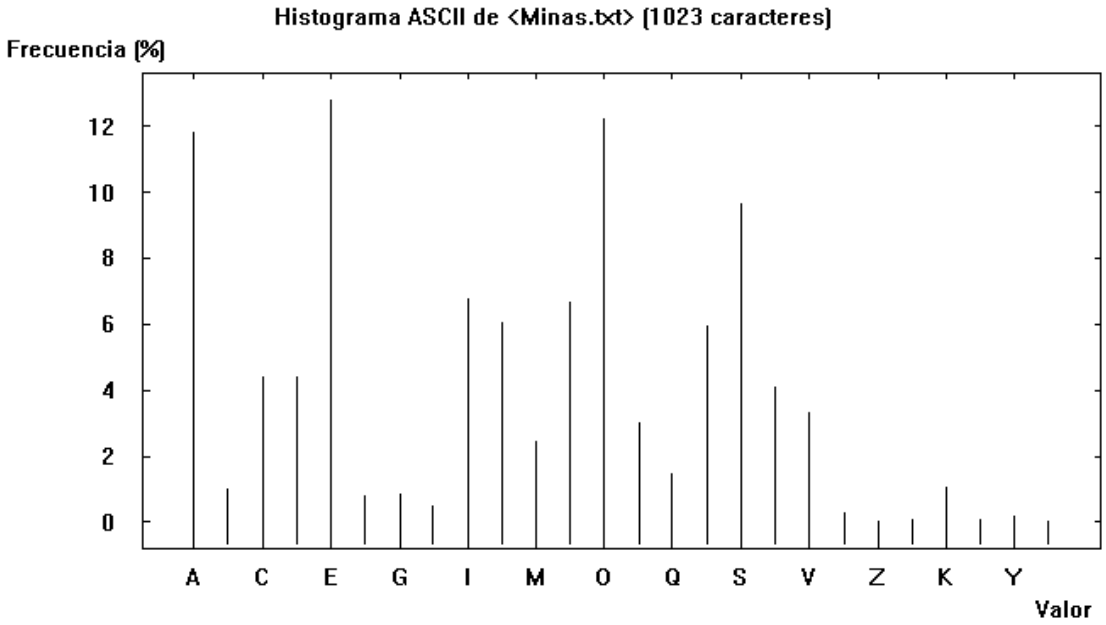


Figura 15. Histograma Minas

En el N-grama los caracteres que tuvieron que ser sustituidos por otros para su inserción en Cryptool se muestran con su valor real, es decir, "rr", "ll" y "ñ":

Histograma Análisis de <Minas.txt>. Tamaño del archivo 1273 bytes.
Ordenados descendentemente por frecuencia.

Nº	Subcadena	Frequencia (en %)	Frecuencia
1	E	12.8055	131
2	O	12.2190	125
3	A	11.8280	121
4	S	9.6774	99
5	I	6.7449	69
6	N	6.6471	68
7	L	6.0606	62
8	R	5.9629	61
9	C	4.3988	45
10	D	4.3988	45
11	T	4.1056	42
12	V	3.3236	34
13	P	3.0303	31
14	M	2.4438	25
15	Q	1.4663	15
16	RR	1.0753	11
17	B	0.9775	10
18	G	0.8798	9
19	F	0.7820	8
20	H	0.4888	5
21	X	0.2933	3
22	LL	0.1955	2
23	Ñ	0.0978	1
24	MG	0.0978	1

Figura 16. N-grama Minas

En este caso se está trabajando con un texto que se encontraba codificado, no cifrado, puesto que no existe clave. Por ello la frecuencia de aparición de los caracteres codificados es de gran ayuda para el descubrimiento de la tabla de codificación. De nuevo, al examinar tanto el histograma como el N-grama se aprecia una diferencia considerable en la frecuencia de aparición de los caracteres, lo que implica que la robustez del sistema no es demasiado buena. Conociendo la lengua en que está escrito y haciendo un estudio del análisis de frecuencias de caracteres, bigramas y trigramas, podría ser fácilmente descodificado.

4.3. DOCUMENTO 3: TEXTO HISTÓRICO DEL SIGLO XVII

A continuación se realiza un estudio de los mismos parámetros (entropía, análisis de frecuencias y autocorrelación) en un texto sin cifrar perteneciente a la misma época de los textos previamente analizados. Este estudio confirma la conclusión a la que se ha llegado sobre la escasa fortaleza y relativa debilidad de los sistemas de cifrado anteriormente estudiados, puesto que los resultados, tanto de entropía como de análisis de frecuencias son bastante parecidos.

Dependiendo del tipo de texto suelen aparecer diferencias notables en cuanto a las frecuencias de las letras, por lo que para este estudio se ha tratado de seleccionar un texto de temática y ámbito similar a los previamente estudiados.

El texto elegido se encuentra en el anexo VII de esta memoria y pertenece a la obra *El aiustamiento y proporcion de las monedas de oro, plata i cobre* de Alonso Carranza, escrita en el año 1629 (22). Alonso Carranza y Tomás Cardona fueron dos arbitristas del siglo XVII; a finales del siglo XVI y principios del siglo XVII comienza a usarse la palabra «arbitrista». En un principio era un término aplicado literalmente a aquél que proponía proyectos, esquemas, «arbitrios», siendo usado para definir a aquellos hombres que idearon todo tipo de esquemas con el intento de contribuir a la restauración política del Imperio español.

El contenido del arbitrio de Carranza es básicamente la defensa de un escrito publicado en 1619 por el capitán sevillano, Tomás Cardona. A grandes rasgos, el proyecto de estabilización presentado por Cardona involucraba como medida un aumento del valor nominal de la plata. Cardona sostenía la opinión, basándose en el contenido de metal precioso en las monedas castellanas, que la moneda de plata estaba subvaluada en Castilla, es decir, que su valor real excedía su valor nominal (opinaba lo mismo con respecto al oro). (23)

El texto, al igual que el de las minas, es un texto formal de carácter político y ambos pertenecen a la misma época.

El aivstamiento i proporción de las monedas de oro, plata i cobre, i la redvcción destos metales a sv debida estimación, son regalia singvlar del rei de España, i de las indias, nvestro señor, qve lo es del oro i plata del orbe.

El capitán thomas de Cardona maestro de sv cámara, i fiscal en la real ivnta de minas.

Desde el año 1600 sin perdonar a trabaxos i desvelos increibles, con no poca costa, insisto en el aivstamiento de las monedas de oro, plata i cobre, i en el avmento de las dos primeras, por diversos memoriales dados a sv magestad, i antes al rei d.phelippe III, nvestro señor que esta en el cielo, i por otros diversos papeles i discvrsos que he divulgado en sv apoio, dando noticia de lo qve con particvlar attencion he observado desde el año de 1580 que tuve edad competente para servir a sv magestad a la milicia de mar i tierra, i navegaciones a las indias. Las quales, i el manexo grande de los thesoros de oro i plata qve vinieron desde aqvel tiempo gran parte a mi cargo, como maestre de plata de las naos de las armadas de la guarda de las indias, capitana i otras mias propias, que vinieron en las armadas del cargo de don francisco coloma, i don luis faxardo, i otros, me fueron advirtiendo i mostrando su perjudicial desperdicio con perdida de mas de quinientos millones, que estos de v.m. han tenido, con utilidad de emulos, i enemigos desta corona.

De la misma forma que en el texto anterior, la "ñ" ha debido sustituirse por otro carácter, para ser aceptada por Cryptool; en este caso se ha reemplazado por "w", obteniendo el siguiente alfabeto para el análisis: ABCDEFGHIJLMNOPQRSTUVXW

- **Entropía**

  La entropía que nos proporciona la herramienta es de 3.92, con una entropía máxima posible de 4.52. De nuevo el valor de la entropía señala una robustez mejorable, resultado bastante lógico, puesto que se trata de un texto en claro que no ha sido cifrado, y el análisis se ha realizado sobre los caracteres del alfabeto normal.

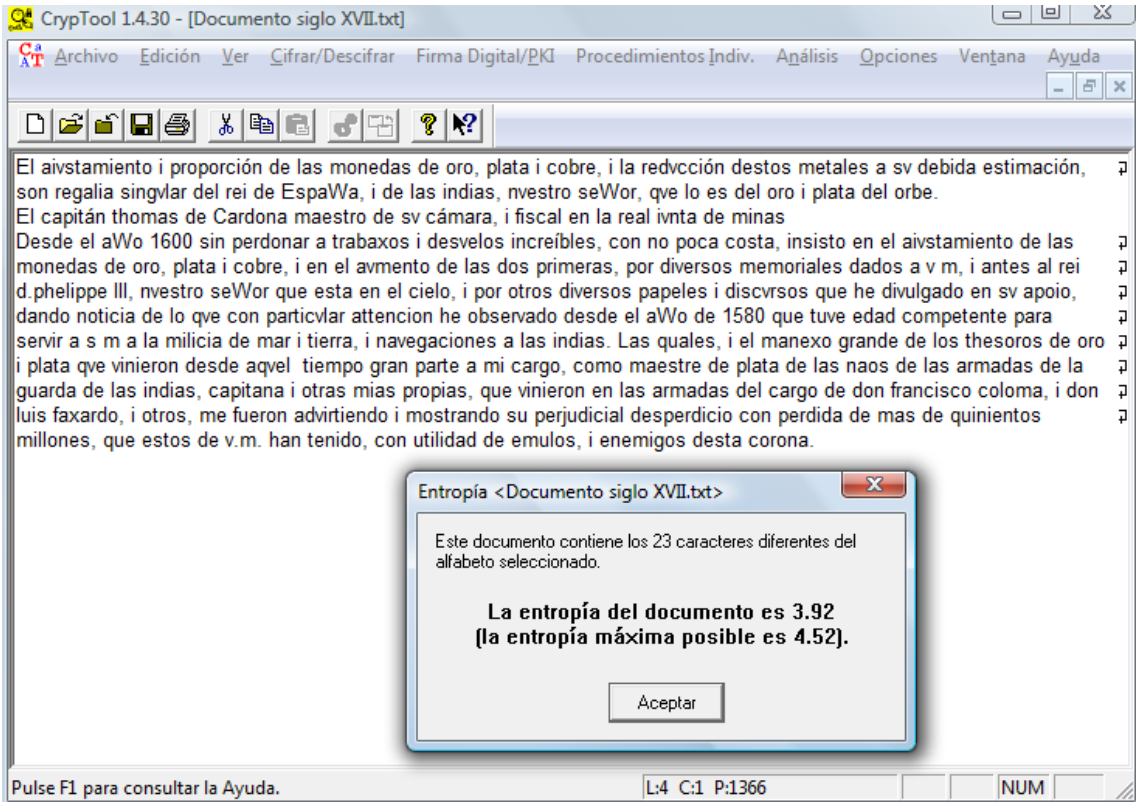


Figura 17. Entropía texto S. XVII

- **Análisis de frecuencias**

Como en los textos anteriores, el análisis de frecuencias se realizará a través del estudio del histograma y el N-grama.

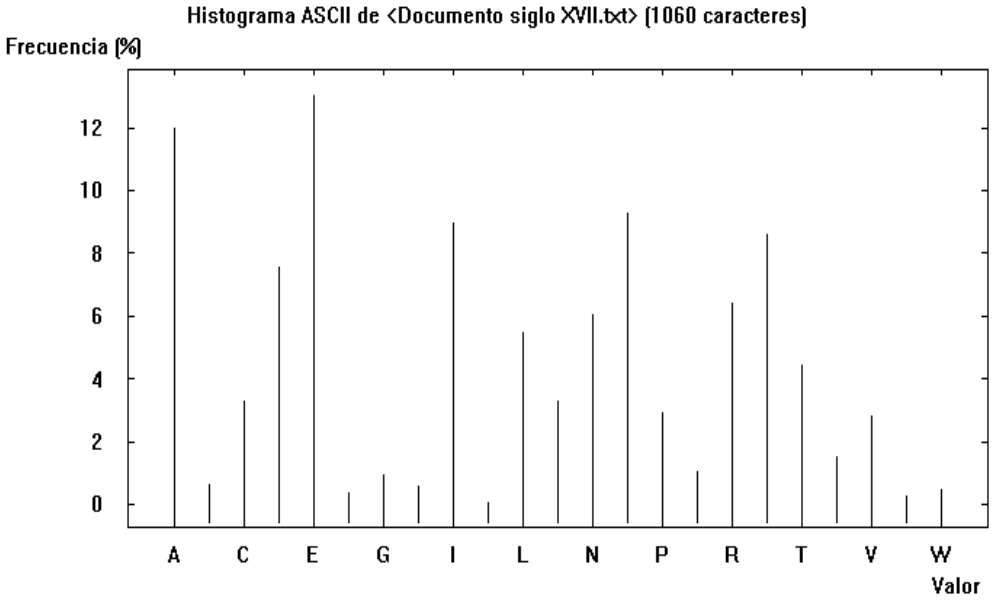


Figura 18. Histograma texto S. XVII

En el N-grama el carácter que tuvo que ser sustituido por otro para su inserción en Cryptool se muestra con su valor real, es decir, "ñ":

Histograma Análisis de <Documento siglo XVII.txt>. Tamaño del archivo 1365 bytes.
Ordenados descendentemente por frecuencia.

Nº	Subcadena	Frequencia (en %)	Frecuencia
1	E	13.0189	138
2	A	11.9811	127
3	O	9.2453	98
4	I	8.9623	95
5	S	8.5849	91
6	D	7.5472	80
7	R	6.4151	68
8	N	6.0377	64
9	L	5.4717	58
10	T	4.4340	47
11	C	3.3019	35
12	M	3.3019	35
13	P	2.9245	31
14	V	2.8302	30
15	U	1.5094	16
16	Q	1.0377	11
17	G	0.9434	10
18	B	0.6604	7
19	H	0.5660	6
20	Ñ	0.4717	5
21	F	0.3774	4
22	X	0.2830	3
23	J	0.0943	1

Figura 19. N-grama texto S.XVII

De nuevo, al examinar tanto el histograma como el N-grama se aprecia una diferencia considerable en la frecuencia de aparición de los caracteres, con la distribución característica de la lengua española.

4.4. ESTUDIO COMPARATIVO DE LOS TRES TEXTOS

A continuación se realiza un estudio comparativo entre los textos previamente analizados. Para ello se comparan las frecuencias de los caracteres más comunes de los textos descifrados, es decir, el texto de las minas y el del siglo XVII. Dichos valores se comparan con los caracteres de mayores frecuencias del texto de Sertori; esta comparación nos permitirá llegar a ciertas conclusiones sobre dicho texto.

Caracteres	Documento Minas	Documento siglo XVII	Mayores frecuencias Sertori
E	12.80	13.01	13.76
A	11.83	11.98	11.47
O	12.21	9.25	10.39
I	6.75	8.96	9.04
S	9.67	8.58	7.02
D	4.40	7.54	5.40
R	5.96	6.42	4.59
N	6.64	6.04	4.45
L	6.06	5.47	4.31
T	6.06	5.47	4.31
C	4.39	3.30	4.18
M	2.44	3.30	3.64
P	3.03	2.92	3.37
V	3.32	2.83	3.24

Figura 20. Tabla comparativa de los tres documentos

En la tabla se observa que los dos textos legibles presentan frecuencias similares en la mayoría de caracteres.

En principio se podría concluir que el texto de Sertori es un texto de sustitución monoalfabética basándonos en el hecho de que el número de caracteres utilizados es prácticamente igual que en el documento de las minas (27 y 26 respectivamente) y en el hecho de que las frecuencias de los caracteres también son bastante similares en ambos sistemas. Sin embargo no se dispone de suficientes datos como para poder afirmarlo; la transformación de los caracteres más comunes por sus supuestas correspondencias y el análisis de los bigramas y trigramas más comunes del texto también ayudarán a descartar o confirmar esta hipótesis.

Si realmente se tratara de un sistema de sustitución monoalfabética, el carácter con la mayor frecuencia representaría la letra "E", el segundo la "A", y así sucesivamente. Si se procede a cambiar los 5 caracteres más comunes por las correspondientes letras, se deberían empezar a apreciar rasgos inteligibles.

Tras realizar esta modificación los caracteres "reales" aparecen en minúscula y en color rojo, siendo el siguiente el texto obtenido:

AYCLiDEAsGRsaResCSisJi KEiOSLMEJooeGDKeMMiiJSsisoaSGDiKJRoaMsa9AeLiOeLiYRSRisiseG
D2CiSALAUoaOoaKJoaeseoECieGAeLoaiMeeoRSEesaieoSJReGEDLiKEDGK20KCe4CsaJEESeLODi
UieROZeGsaJeoaoSJZDK5AeiSeiee6GsaJeRSsaJJeoaoKIADOCKe4s3SJoaoaSLJeoesaGeiJieosaRe
AaDSeAeeoDeAeoeoaReSK8eCisaLEADUsaoaUeoasASKSeLD24EAKGAsaeeoSJsaei555DsaGCio
aJoaAMMioaKRSLieoRSsaeisaG5ESDsa2eoCSKAsaLUKioaeoOGRKJoaUDsaCi8KeDUieoeRsaDA
GAGoa2oaeoSiR2AeisaDKeSaReDseoKD8saesoaUR2isaGSsseDi8iJJeoSoaeeoSi2aZsaeDeSaKLaJ
saoaeieoeSGSaRiDKeAsaKLaioaKeEDEiesaXSRsaLieiLXisaGoaLDeossaeiL8LeXLSKioa5DsaZSeR2
GALZAsaLKieeoEiJRieoKSaEooooaYLeGLiJMiMSeoAiAeLRoaEeKiREeAeoeoYAeoaoai2DLeoiARi
EJoa5Ksa5DAeooa2AJKiEiMC8SEoaSLDsaGAiRYeiJeoDiRsaieLooeGEKieKoaoaReSLoooasaRYe
AARieoeEGKoaeSLaDRsaXoaiAeCiYeGJeoEeL

Si bien muy al principio del texto transformado podría parecer que efectivamente se trata de un texto de sustitución monoalfabética, enseguida se descarta dicha hipótesis puesto que aparecen muchas vocales seguidas, llegando incluso a cinco. Aun así se plantean las frecuencias correspondientes a los bigramas y trigramas más comunes:

Digrama Análisis de <Sertori.txt>.
Ordenados descendentemente por frecuencia.

Nº	Subcadena	Frequencia (en %)	Frecuencia
1	B3	5.1771	38
2	F3	5.1771	38
3	NB	4.4959	33
4	PN	2.0436	15
5	3N	1.6349	12
6	AN	1.4986	11
7	NP	1.3624	10
8	PF	1.2262	9
9	BB	1.0899	8
10	BN	1.0899	8
11	NG	1.0899	8
12	NL	1.0899	8

Figura 21. Digramas texto Sertori

A la vista de esta tabla y según las correspondencias de la figura 21, los 3 bigramas más comunes serían “oa”, “sa” y “eo”, que obviamente no son palabras del alfabeto español.

Trigrama Análisis de <Sertori.txt>.
Ordenados descendentemente por frecuencia.

Nº	Subcadena	Frequencia (en %)	Frecuencia
1	PNB	0.9629	7
2	B3N	0.8253	6
3	F3G	0.8253	6
4	F3N	0.8253	6
5	JNB	0.8253	6
6	NBN	0.8253	6
7	3B3	0.6878	5
8	3RN	0.6878	5
9	B3B	0.6878	5
10	DF3	0.6878	5
11	JB3	0.6878	5
12	NB3	0.6878	5

Figura 22. Trigramas texto Sertori

Procediendo de igual manera para los trigramas más frecuentes, estos deberían ser "ieo", "oae" y "sae".

Todos estos datos en principio nos llevarían a afirmar que no se trata de un sistema de sustitución monoalfabética.

Se plantea por tanto la posibilidad de que se trate de un sistema de cifrado polialfabético. El método por excelencia de sustitución polialfabética de la época es el cifrado de Vigenère. Volviendo a la autocorrelación obtenida en el apartado 4.1., se utilizará este parámetro para calcular la longitud de la clave supuestamente utilizada para el cifrado del texto:

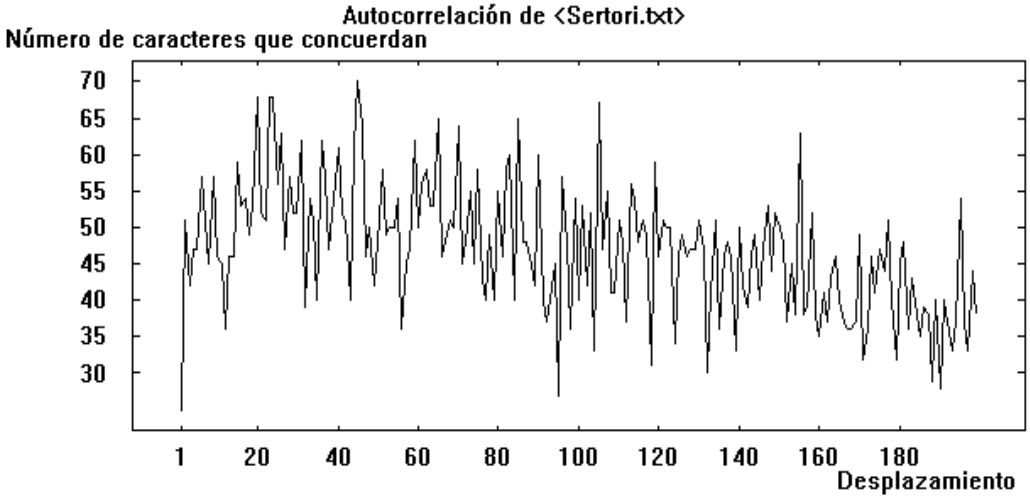


Figura 23. Autocorrelación texto Sertori

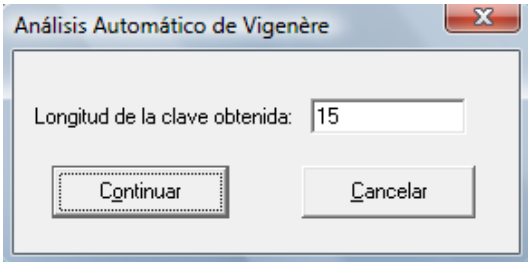


Figura 24. Longitud de la clave en cifrado de Vigènere

La herramienta nos proporciona la clave utilizada (FBBJ888JJ0JBUFU) y su longitud: 15.

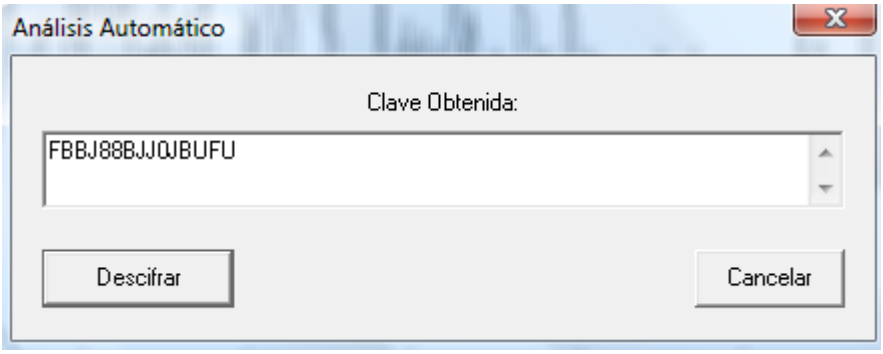


Figura 25. Clave en cifrado de Vigènere

Para aceptar como válida o descartar esta hipótesis se continúa con el análisis proporcionado por Cryptool, cuyo siguiente paso es la presentación del texto descifrado:

4XBCUGDY8IIEEL4ABRGJMOB5RFR2GPDAAEKGJEDNGOXMRKEAOYKCGB
KIAEGRS80EOUNECRMP0L8AOEEKGY3GUYKLNMSNAONMAOEGEAP88IF0
EOE2GDOEA9MPIE2GRERAIO9DOF8EDC9N59B3OPBRSX0DREOSCGKREP5ZI
SA2IEE8AJAZEB4LI8MMOER6KEOAOIRRSXDMAOENGY4P3J4URSRI28E2JCK
EA4AEBMOAURA8OSE0E90I0MEEGMYECEAEL4MJ5EFUEOCFYCAAE52SEE8
EYJLJM29DUD0BKDEOEO2RXAEIO4R0GEO9DGAEDMS0LDUE2BIUCO459ME
2EUJ29RFJCRSDIABJNDEOCXBOMS45NFINMAOKE82NKIEMCKURAEIGOCL
BLBA2NE8M2JRIYLI8A2CBRY2IEE8MMEOYE2EJE2KI3GEEB0AEM4UAOAAO

2RMS4IARG58ZEOEEEREE2SIEOE8MGECERSMELOCBRDEOBMOOMSYIDC5
UREOLUIEEF8IOKLUJ2924CC45RA2MGOAKELMJJ85EXCEOZYRPN9BCZ0RS2
EOMEEIOAIREAYME0AA2E8XCEICOXG8GRM2DU0ECS22PIYKPDEDRAE22Y
MMSMSOY4ORAGYSGDX5EXJEO0G0E2COYLDYKDODFAR524JKOAEB0OI4
ROAEC4O9AEKMK2ERF5BREJMSMSPMJOEA2OGOPCIL4POEERD9BCOM0FE
9PEO3E2GYO3OCISDMA5RO

Con este nuevo texto se realiza de nuevo un estudio de las frecuencias de los caracteres en él presentes, obteniendo:

Histograma Análisis de <Análisis Automático de Vigenère de <Sertori.txt>, clave: <FBBJ88BJJ0JBUFU>>.
Ordenados descendentemente por frecuencia.

Nº	Subcadena	Frequencia (en %)	Frecuencia
1	E	14.3050	106
2	O	8.5020	63
3	A	6.6127	49
4	R	5.8030	43
5	M	5.6680	42
6	2	4.8583	36
7	I	4.5884	34
8	C	4.0486	30
9	G	3.9136	29
10	D	3.6437	27
11	S	3.2389	24
12	B	2.9690	22
13	8	2.8340	21
14	K	2.8340	21
15	Y	2.8340	21
16	J	2.6991	20
17	4	2.5641	19
18	0	2.4291	18
19	L	2.1592	16
20	U	2.1592	16
21	5	2.0243	15
22	9	1.8893	14
23	P	1.8893	14
24	N	1.7544	13
25	F	1.4845	11
26	X	1.4845	11

Figura 26. Texto descifrado con Vigènere

En este caso, las frecuencias son muy diferentes a las esperadas; no se encuentran en el mismo margen de valores que las de los otros dos documentos analizados, por lo que se puede concluir que Vigènere tampoco es el sistema de cifrado utilizado. Este resultado era relativamente esperado, puesto que el cifrado de Vigenère

es quizá demasiado moderno para ser utilizado en este documento. Además supondría un "doble cifrado", puesto que tras aplicar Vigenère, se habría codificado el resultado con una tabla de símbolos.

Por tanto, volvemos a plantear la hipótesis inicial de que efectivamente se trate de un sistema de sustitución monoalfabético. Existen dos datos relevantes que nos llevan a esta conclusión:

1. El número de caracteres utilizados en los otros documentos y en el de Sertori es prácticamente igual.

2. Como se puede apreciar en la figura 20, las frecuencias de aparición de los caracteres son muy similares en los tres documentos. Este resultado no sería el esperado si un sistema de cifrado distinto fuese utilizado.

El hecho de que los resultados al descodificar no sean los esperados, puesto que no se encuentran indicios de palabras con sentido, podría deberse a un pequeño desajuste de las frecuencias. Al fin y al cabo se trata de un texto antiguo cuya visibilidad era insuficiente y del que no se disponía previamente del alfabeto utilizado. Además el texto completo consta de 741 caracteres, que podría resultar insuficiente para afirmar que se trate de uno u otro sistema.

Estos pequeños desajustes son menos relevantes que los dos datos anteriormente mencionados, que son claros indicadores de que efectivamente se trata de un sistema de sustitución monoalfabética.

CAPÍTULO 5

CONCLUSIONES Y LÍNEAS FUTURAS DE INVESTIGACIÓN

5. CONCLUSIONES Y LÍNEAS FUTURAS DE INVESTIGACIÓN

Después del análisis realizado en la sección anterior, se plantearán en este apartado posibles futuras líneas de investigación y las conclusiones que se han alcanzado.

5.1. LÍNEAS FUTURAS DE INVESTIGACIÓN

Tras estudiar ambos textos, y la robustez de los sistemas utilizados, se plantean varias posibles líneas futuras de investigación.

Obviamente, al tratarse de documentos de los siglos XVI y XVII, hoy en día ambos sistemas podrían ser ampliamente mejorados.

El siguiente avance lógico en el estudio de estos textos sería su desciframiento, basándose en los análisis de frecuencias realizados y en un estudio paralelo del idioma y el contexto histórico del documento.

Como se ha mencionado en el apartado anterior, el texto de Sertori presenta características propias de los sistemas de sustitución monoalfabética, por lo que en principio se puede concluir que podría ser descifrado realizando un estudio minucioso de las frecuencias, no solo de los caracteres, sino de bigramas y trigramas. Los desajustes que se mencionaban en el apartado anterior podrían desaparecer si se plantearan varias hipótesis. El texto es de extensión bastante reducida por lo que podría suceder que lo que estamos considerando como el carácter más frecuente, en realidad fuese el segundo más frecuente. Es decir, se debería jugar un poco cambiando los caracteres que presentan frecuencias similares con el fin de obtener un texto mínimamente inteligible.

En cuanto al documento de las minas, se trata de un documento bastante extenso. Para el cometido de este proyecto, que era analizar las características del sistema de cifrado utilizado, bastó con descifrar un par de páginas del documento. Una posible

futura línea de investigación sería el desciframiento del texto completo, que consta de unas treinta páginas.

Una vez descifrados ambos documentos se podría realizar un estudio comparativo entre los sistemas utilizados para cifrarlos y otros sistemas utilizados en la época, analizando diferencias y semejanzas, así como ventajas e inconvenientes de cada uno de los sistemas. Un análisis interesante sería la comparación entre estos sistemas y las cifras utilizadas en los reinados de Felipe II y Felipe III, puesto que pertenecen a la misma época que los documentos analizados en este proyecto. Alguna de estas cifras se muestra en los anexos de esta memoria.

Otra posible línea de investigación sería el análisis comparativo de estos sistemas de cifrado de los siglos XVI y XVII con los utilizados en la actualidad. Pese al obvio avance tecnológico experimentado por los sistemas de cifrado, los sistemas de una y otra época separadas por cuatro siglos, presentan un gran número de puntos en común.

Al margen de los documentos utilizados para el estudio de este proyecto, el procedimiento utilizado podría ofrecer la posibilidad de recuperación de muchos documentos o fragmentos de diversas épocas que siguen cifrados. En los casos en que la recuperación total del texto original no fuera posible, como mínimo proporcionaría una nueva perspectiva de análisis de la robustez, capacidad y parámetros de análisis criptológico.

5.2. CONCLUSIONES

La principal conclusión general de este proyecto es que la investigación interdisciplinar entre historiadores de la criptografía e informáticos que aquí se plantea podría suponer la recuperación de textos cifrados inéditos pertenecientes a distintas épocas históricas.

A lo largo de toda la sección anterior se puede observar cómo la información sobre los datos históricos de los documentos y los métodos vistos en el recorrido histórico de la criptografía complementan la información proporcionada por la

herramienta informática utilizada para el análisis de los textos. La investigación basándonos tan solo en una de las disciplinas habría proporcionada unos resultados distintos, insuficientes e incompletos.

En cuanto a las conclusiones concretas sobre los textos analizados, sintetizaremos en este apartado los resultados obtenidos en la sección anterior y las conclusiones a las que nos conducen:

La falta de contexto del primer documento analizado (se sabe tan solo que pertenece al siglo XVI y que su creador fue Gerónimo Sertori) y la difícil visibilidad que en ocasiones presenta, han dificultado el estudio de este texto, sobre todo a la hora de crear un abecedario sobre el que basar su análisis. Sin embargo, tras realizar las transformaciones, cálculos y comparaciones pertinentes, los datos sugieren que se trata de un sistema de sustitución monoalfabética o simple, en el que cada caracter del texto original es sustituido por otro, siguiendo una tabla preestablecida de correspondencias.

Del segundo documento analizado, el texto de las minas del siglo XVII, se disponía de más contexto, tanto de su autor como de las circunstancias en que fue escrito, así como la fecha exacta de su creación. La gran dificultad de este documento ha sido descifrarlo, puesto que, como se puede apreciar en el anexo de esta memoria, no solo se han de tener en cuenta los símbolos sino la posición exacta que estos ocupan. Se trata de un sistema de sustitución monoalfabética, y los resultados obtenidos en su análisis han sido más o menos los esperados.

El análisis del tercer documento, que no se encontraba cifrado, ha sido clave para alcanzar estas conclusiones, puesto que ha proporcionado la base fiable con la que comparar los otros documentos que datan de la misma época.

BIBLIOGRAFÍA Y REFERENCIAS

BIBLIOGRAFÍA Y REFERENCIAS

1. **RAE (Real Academia de la Lengua Española).** *Diccionario de la lengua española.*

2. **Ramió Aguirre, Jorge.** *Seguridad Informática y Criptografía.* Madrid : s.n., 2006.

3. **Universidad de Zaragoza.** *Criptografía Clásica (Criptografía y Seguridad en Redes de Comunicaciones) http://criptosec.unizar.es/doc/tema_c1_criptosec.pdf.*

4. **SABIA (Sistemas Adaptativos y Bioinspirados en Inteligencia Artificial).** *Criptografía. Definiciones y Conceptos previos.* Teconologías de la Información y las Comunicaciones, Universidad de La Coruña. http://sabia.tic.udc.es/docencia/ssi/docs/transparencias/Criptografia.clave.privada.pdf.

5. **Ribagorda Garnacho, Arturo.** *Intypedia. Information Security Encyclopedia. Historia de la Criptografía y su desarrollo en Europa.* Madrid : s.n., 2010. http://www.criptored.upm.es/intypedia/docs/es/video1/GuionIntypedia001.pdf.

6. **CSIC (Consejo Superior de Investigaciones Científicas).** *Línea del Tiempo / un viaje a través de la historia de la criptografía y el criptoanálisis.* Departamento de Tratamiento de la Información y Codificación. http://www.iec.csic.es/cryptool/menu_zeittafel.es.html.

7. **Galende Díaz, Juan Carlos.** *Criptografía. Historia de la escritura cifrada.* Madrid : Editorial Complutense, 1995.

8. **Fouché Gaines, Helen.** *Cryptoanalysis: a study of ciphers and their solution.* New York : Dove Publications, 1956.

9. **García del Castillo, Crespo C, Ortega Triguero, Jesús J y López Guerrero, Miguel Ángel.** *Introducción a la Criptografía. Historia y Actualidad.* s.l. : Ediciones de la Universidad de Castilla la Mancha, 2006.

10. **Quirantes Sierra, Arturo.** *La Cifra General de Felipe II.* Taller de Criptografía. Universidad de Granada. http://www.ugr.es/~aquiran/cripto/museo/felipeii-1556.htm.

11. **Devos, J.P.** *Les chiffres de Philippe II et du Despacho Universal durant le XVII siecle.* Bruselas : s.n., 1950.

12. **Navarro Bonilla, Diego.** *Lor Archivos del Espionaje: Información, Razón de Estado y Servicios de Inteligencia en la monarquía hispánica.* Salamanca : Caja Duero, 2004.

13. **Quirantes Sierra, Arturo.** Boletín Enigma 77. [En línea] 2010. http://www.cripto.es/enigma/boletin_enigma_77.txt.

14. **Núñez Contreras, Luis.** *Manual de paleografía. Fundamentos e Historia de la escritura latina.* Madrid : Cátedra, 1994.

15. **Ministerio de Cultura.** Archivo General de Simancas. [En línea] http://www.mcu.es/archivos/MC/AGS/Presentacion.html.

16. **Xifré Solana, Patricia.** *PFC: Antecedentes y perspectivas de estudio en historia de la Criptografía.* 2009.

17. **Ramió Aguirre, Jorge.** Intypedia (Information Security Encyclopedia). [En línea] 2010. http://www.intypedia.com/.

18. **Bernal, Rodríguez Antonio Miguel.** *España, proyecto inacabado. Costes/beneficios del imperio.* Madrid : Ediciones Marcial Pons, 2005.

19. *Cifras y claves indianas.* **Lohmann, Guillermo.** Sevilla : s.n., 1954, Anuario de estudios americanos, Vol. XI.

20. **Web oficial de Cryptool.** Introducción a Cryptool. [En línea] http://www.cryptool.com/index.php/es.html.

21. **Fletcher Pratt, Murray.** *Secret and Urgent: the Story of Codes and Ciphers.* s.l. : Blue Ribbon Books, 1939.

22. **Carranza, Alonso.** *El Aiustmiento I Proporcion de las monedas de oro, plata I cobre.* Madrid : s.n., 1629. Biblioteca Nacional Madrid, Raros: 34521..

23. **de Lozanne Jefferies, Claudia.** *Un proyecto de estabilización monetaria con expectativas adaptativas en Castilla del Siglo XVII. El arbitrio de Francisco Antonio de Alarcón (1642). Universidad de Santiago de Compostela.*

24. **Colegio Oficial de Ingenieros Técnicos de Telecomunicaciones.** *Orientanción al libre ejercicio. Honorarios profesionales.* 2010.
http://www.coitt.es/res/libredocs/Honorarios.pdf.

ANEXOS

ANEXOS

En este último apartado de la memoria incluimos algunos de los documentos citados, analizados o que han intervenido en la elaboración de este proyecto.

I. PRESUPUESTO

El presupuesto para la realización de este proyecto está formado por los honorarios del Ingeniero Técnico de Telecomunicaciones que realiza el estudio, y el coste de los equipos, software y material que este necesita para su desarrollo.

Conviene aclarar que, puesto que el proyecto no consiste en la creación de un software para su posterior venta, sería más preciso hablar de costes que de presupuesto, limitándose este apartado a detallar cada uno de los costes individuales que han surgido en el desarrollo del proyecto.

El ritmo de trabajo de los nueve meses transcurridos desde la asignación del proyecto no ha sido constante, pero se puede hacer un cálculo aproximado para computarlo con vistas al presupuesto total de proyecto. De media se ha trabajo unas 4 horas al día; tras descontar festivos, vacaciones, fines de semana y periodos de menor actividad, el número aproximado de horas totales dedicadas al proyecto es de 540. En cuanto a los honorarios oficiales, estos ya no aparecen en la página del Colegio Oficial de Ingenieros Técnicos de Telecomunicación, puesto que el Ministerio de Economía y Hacienda remitió a todos los colegios profesionales una nota en la que se recordaba que, siguiendo directivas europeas, se debían eliminar los baremos orientativos de honorarios que tradicionalmente se venían publicando. En dicha nota se hacía constar que los honorarios son libres y responden al libre acuerdo entre el profesional y su cliente (24). Por lo tanto, para el cálculo del presupuesto y basándonos en los últimos datos de que se tiene constancia, se ha establecido un valor orientativo 65€/hora.

Por lo tanto los costes pueden verse en la siguiente tabla:

PERSONAL:

Concepto	Nº de horas	Honorarios	Importe
Ingeniero Técnico de Telecomunicaciones	540	65 euros/hora	**35100**

Con respecto a los programas utilizados, básicamente han sido Cryptool, Microsoft Office (Word, Excel y Picture Manager) y el programa de manipulación de imágenes GIMP.

Cryptool es una herramienta de libre distribución para apoyo a la docencia sin coste adicional alguno; GIMP también es un programa gratuito. Los costes del resto de los programas se pueden observar en la siguiente tabla:

SOFTWARE:

Programa	Coste Licencia (euros)
Cryptool	0
Microsoft Office 2007	139.00
ISTS JPEG to PDF Creator	0
TOTAL	**139.00**

Los equipos utilizados han sido un ordenador portátil con licencia del sistema operativo Windows Vista, un ordenador de sobremesa con licencia del sistema operativo Windows XP y una impresora multifunción.

EQUIPOS:

Programa	Coste sin IVA (Euro)	% Uso dedicado proyecto	Dedicación (meses)	Periodo de depreciación	Coste imputable*
Ordenador portátil HP Pavilion DV2	630.00	75	9	36	140.62
Ordenador de sobremesa LG	672.00	20	9	72	17.5
Impresora HP PSC 2355	116.76	25	9	60	5.21
				TOTAL	**163.33**

* Fórmula de cálculo de la amortización:

$$\frac{A}{B} xCxD$$

A = nº de meses desde la fecha de facturación en que el equipo es utilizado
B = periodo de depreciación
C = coste del equipo (sin IVA)
D = % del uso que se dedica al proyecto

Entre los costes indirectos del proyecto se incluyen gastos de material de oficina (tinta y papel), conexión a Internet, electricidad, transporte etc., y suponen un importe aproximado de 200€.

A continuación se resumen los costes totales con el IVA añadido en los casos en que sea necesario, es decir, en los costes de software y de equipos.

RESUMEN DE COSTES

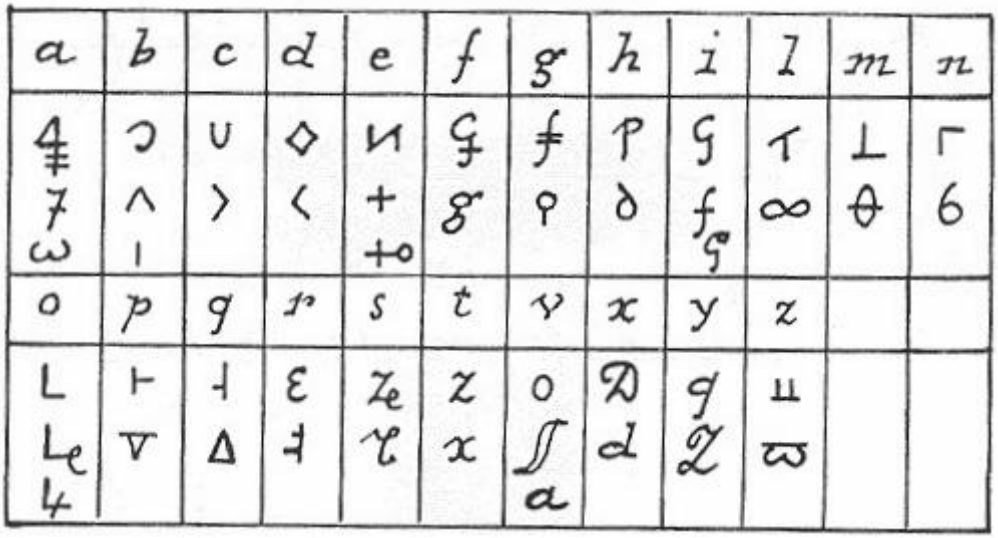
Concepto	Costes totales
Personal	35100
Software	164.02
Equipos	192.73
Gastos indirectos	200
Total	**35656.75**

II. CIFRA GENERAL DE FELIPE II

La Cifra General de 1556 está datada en Gante, a 8 de Noviembre de 1556, y según David Kahn, fue uno de los mejores sistemas de su tiempo. Se compone de tres partes: un vocabulario de sustitución monoalfabética con homófonos (donde cada letra podía ser sustituido por un signo, a escoger entre varios); un silabario (para cifrar grupos de dos o tres letras); y un diccionario de términos comunes.

La Cifra General original se guarda en el Archivo de Simancas. La copia que aquí se presenta está sacada de la compilación de J.P. Devos (*Les chiffres de Philippe II (1555-1598) et du Despacho Universal durant le XVIIe Siecle*, 1950).

- **Vocabulario**: vocabulario de sustitución donde cada letra podía ser sustituido por un signo a escoger entre varios.

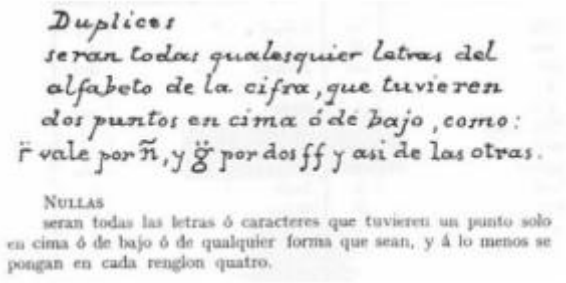


- **Silabario**: sistema para cifrar grupos de dos o tres letras

ba	be	bi	bo	bu
m-	m	-m	m+	me
11	12	13	14	15
da	de	di	do	du
e-	é	-e	e+	ee
21	22	23	24	25
ga	ge	gi	go	gu
9-	9	-9	9+	9e
31	32	33	34	35
ja	je	ji	jo	ju
◇-	◇	-◇	◇+	◇e
41	42	43	44	45
ma	me	mi	mo	mu
ω-	ω	-ω	ω+	ωe
51	52	53	54	55

ca	ce	ci	co	cu
n-	n	-n	n+	ne
16	17	18	19	20
fa	fe	fi	fo	fu
a-	á	-a	a+	ae
26	27	28	29	30
ha	he	hi	ho	hu
b-	b	-b	b+	be
36	37	38	39	40
la	le	li	lo	lu
s-	s	-s	s+	se
46	47	48	49	50
na	ne	ni	no	nu
o-	ó	-o	o+	oe
56	57	58	59	60

- **Duplices**



Duplices
seran todas qualesquier letras del alfabeto de la cifra, que tuvieren dos puntos en cima ó de bajo, como: r̈ vale por ñ, y g̈ por dos ff y asi de las otras.

NULLAS
seran todas las letras ó caracteres que tuvieren un punto solo en cima ó de bajo ó de qualquier forma que sean, y á lo menos se pongan en cada renglon quatro.

- **Diccionario** para la codificación de términos comunes

A		adonde	it
Alemania	ab	aun	ot
Alemanes	eb	**B**	
Argel	ib		
Africa	ob	Beatitud	ut
Alexandria	ub	Bohemia	ba
armas	al	baxa	be
armada	el	Bugía	bi
artilleria	il	Berbería	bo
arcabuzes	ol	Barcelona	bu
amigo	ul	Bonifacio	bla
amistad	am	batalla	ble
año	em	batería	bli
aviso	im	bastimentos	blo
amotín	om	bastante	blu
aca	um	**C**	
aquí	ar		
alla	er	Cartagena	bra
allí	ir	Cerdeña	bre
ay	or	Corcega	bri
assí	ur	Calabria	bro
ante	at	Constantinopla	bru
allende	et	Corfu	bal

Candía	bel	Dorguí	dri
ciudad	bil	daño	dro
castillo	bol	designo	dru
campo	bul	despach	dal
campaña	ca	dinero	del
Christiandad	ce	diligencia	dil
carestía	ci	donde	dol
cardenal	co	despues	dul
concilio	cu	desde	dar
collegio	cla	de manera	der
consejo	cle		
capitan general	cli	**E**	
capitan	clo	emperador	dir
coronel	clu	España	dor
cavallos	cra	Españoles	dur
cavalleria	cre	Escocia	das
carta	cri	embaxador	des
correo	cro	embaxada	dis
compania	cru	exercito	dos
casa	cam	effecto	dus
capítul	cem	empresa	fa
correspon	cim	enemigo	fe
como	com	estado	fi
con	cum	espia	fo
		escrí	fu
D		esto	fla
		ello	fle
Díos	car	esta	fli
Duque de Saboya	cer	ella	flo
Duque Octavio	cir	esendo	flu
Duque d'Alva	cor		
Duque de Cleves	cur	**F**	
Duque de Florencia	da		
Duque de Ferrara	de	Flandes	fia
Duque de Mantua	di	Francia	fie
Duque de Urbino	do	Franceses	fii
Duque	du	Florencia	fio
Duquesa	dra	Florentin	fiu
Ducado	dre	Ferrara	fal

frontera	fel	hombre	gar
fragata	fil	humíl	ger
flota	fol	hasta	gir
Frisica	ful		
fruto	fam	I	
Frisia	fem	imperio	gor
fama	fim	Italia	gur
favor	fom	Italianos	ha
fortifier	fum	Inglaterra	he
Fez	far	Ingleses	hi
fin	fer	India	ho
firme	fir	isla	hu
forma	for	infanteria	hal
		Infantes	hel
G		importante	hil
Genova	fur	import	hol
Ginoveses	ga	instructíon	hul
Grecia	ge	impedimento	ham
Grisones	gi	intencíon	hem
Goleta	go	inteligencía	him
galeota	gu	Iusticia	hom
gente	gla	Iuez	hum
guerra	gle	inicio	har
general	gli	iuntamente	her
guarda	glo		
galera	glu	L	
govierno	gra	Lombardia	hir
govern	gre	Levante	hor
gast	gri	La romania	hur
grande	gro	La marca	has
guarnícion	gru	La moria	hes
		Lucano	his
H		Luqueses	hos
honrra	gal	legado	hus
herman	gel	liga	la
hecho	gil	Luteranos	le
hiziese	gol	ley	li
hareis	gul	libertad	lo

libre	lu
lugar	lam
lexas	lem
luego	lim
legua	lom
licencia	lum
loqual	lar
laqual	ler
losquales	lir
lasquales	lor
loque	lur
leri	las
larg	les
limit	lis

M

mundo	los
marques	lus
Milan	lat
Milaneses	let
Mallorca	lit
Menorca	lot
Malaga	lut
Marsella	ma
Malta	me
Mecina	mi
Monago	mo
monasterio	mu
Moros	mal
mar	mel
marina	mill
muralla	mol
mill	mul
milicia	man
municion	mem
ministro	mim
mantenimj^{o} (1)	mon

(1) mantenimiento

merced	mun
memoria	mar
mutín	mer
manera	mir
más	mor
mes	mur
mayor	mas
mejor	mes
menester	mis

N

Napoles	mos
Napolitanos	mus
Navarra	na
Negroponte	ne
Niça	ni
nuncio	no
negocio	nu
nave	nal
necessidad	nel
necessario	nil
negligencia	nol
nuestro	nul
nuestra	nam
no obstante	nem
numero	nim
nosepu	nom
nunca	num

O

Orbitelo	nar
Otranto	ner
obispo	nír
oportunidad	nor
obligacion	nur
obliga	nas
ofrescimiento	nes
ofresc	nis

occasion	nos	quan	quíl
ocurre	nus	quanto	quol
orden	pa	quantidad	quul
officio	pe	qual	quam
obediencia	pi	qualídad	quem
obede	po	question	quím
occupacion	pu	quasí	quom
occup	pla		
P		**R**	
		Roma	quum
Papa	ple	rey	quar
principe	pli	reyna	quer
Principe de España	plo	reyno	quir
Principe Andrea Doria	plu	Rey de España	quor
potentado	pra	Rey de Inglaterra	quur
Portugal	pre	Rey de Romanos	quas
Portugueses	pri	Rey de Francia	ques
Piamonte	pro	Rey de Portugal	quis
Pomblín	pru	Rey de Bohemia	quos
Pulla	pal	Reyna de Escocía	quus
puerto	pel	Rey de Polonia	ra
Puerto Hercules	pil	Rey de Dinamarca	re
provincia	pol	Rey de Tunez	ri
principal	pul	Rey de Argel	ro
persona	pam	Ragusa	ru
polvora	pem	Reverendissimo	ral
pílota	pim	religíon	rel
pacific	pom	republíca	ril
paz	pun	razón	rol
provision	qua	remedío	rul
prone	que	resolucíon	ram
para	qui	resolví	rem
paraque	quo	respuesta	rim
porque	quu	**S**	
pero	qual		
Q		Santopadre	rom
		Su Santidad	rum
quando	quel	Su Beatitud	ras

Su Magestad	res
Su Alteza	ris
Su Excellencia	ros
Sede Apostolica	rus
Serenisimo	rat
Serenisima	ret
Saboya	rit
Suiça	rot
Suiços	rut
Sicilia	ta
secta	te
secretario	ti
secret	to
señor	tu
señoria	tra
satisfaction	tre
sazón	tri
socorro	tro
suma	tru
sucesso	tam
servicio	tem
siempre	tim
T	
Toscana	tom
Trento	tum
Turquía	tas
Turco	tes
Tunez	tis
tierra	tos
tregua	tus
trigo	va
trato	ve
tractado	vi
todo	vo
toda	vu
tanto	val
tanta	vel
tiempo	vil

V	
Vuestra Magestad	vol
Vuestra Alteza	vul
Vuestra Excellencia	vam
Vuestra Señoria	vem
Vuestra merced	vim
Virey de Napoles	vom
Virey de Sicilia	vum
Virey de Cataluña	vaz
Virey de Navarra	vez
Virey de Cerdeña	viz
Virey de Mallorca	voz
Virey de Menorca	vuz
Venecia	vas
Venecianos	ves
Ungria	vis
Ungaros	vos
Villafranca	vus
villa	xa
verdad	xe
vírtud	xi
vitoria	xo
vitualla	xu
Vizcocho	xal
vandera	xel
vela	xil
vuestro	xol
vuestra	xul
unión	xam
unído	xem
unída	xom
Z	
Zante	xim
zabra	xon

III. CIFRA PARTICULAR DE 1568

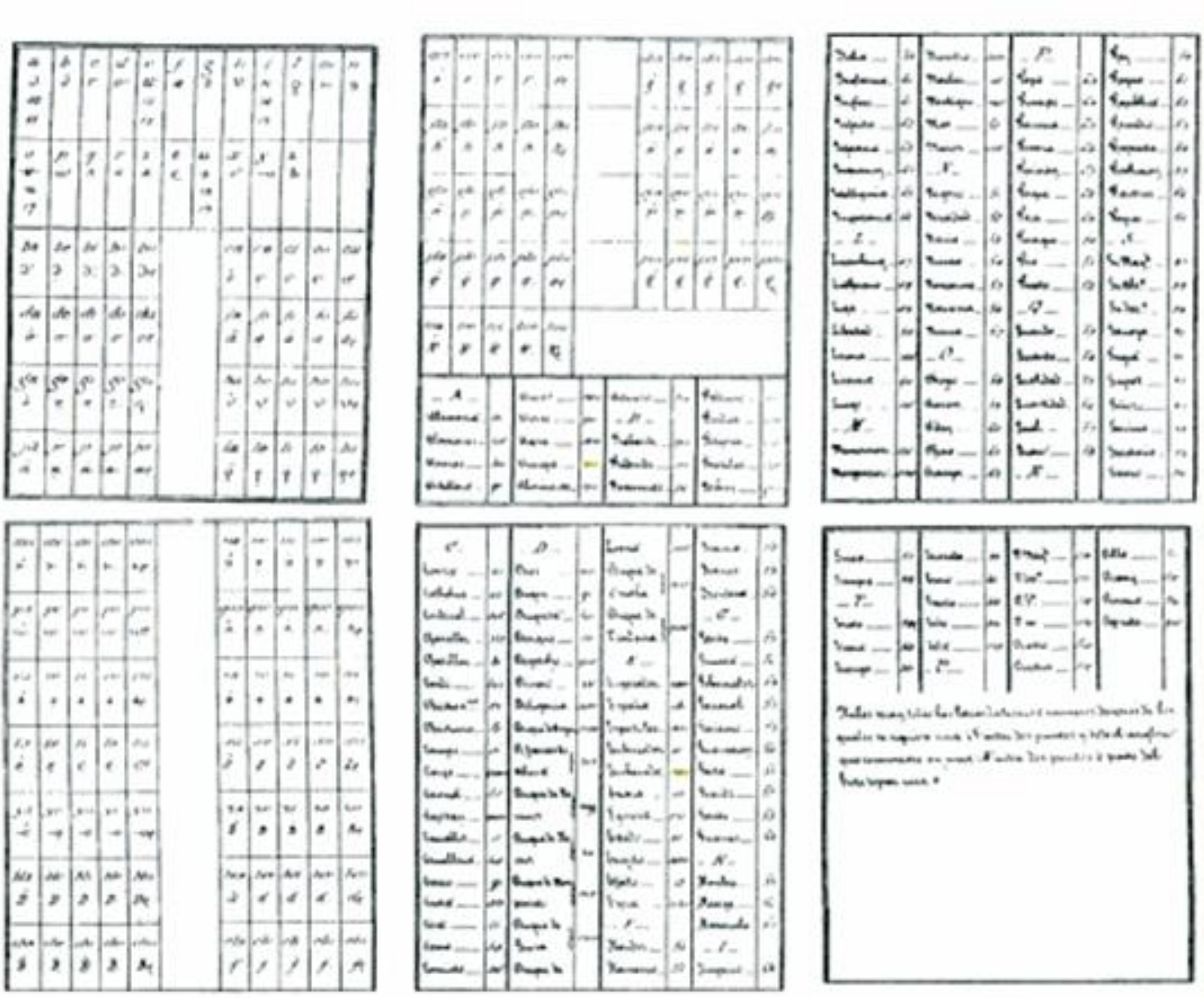
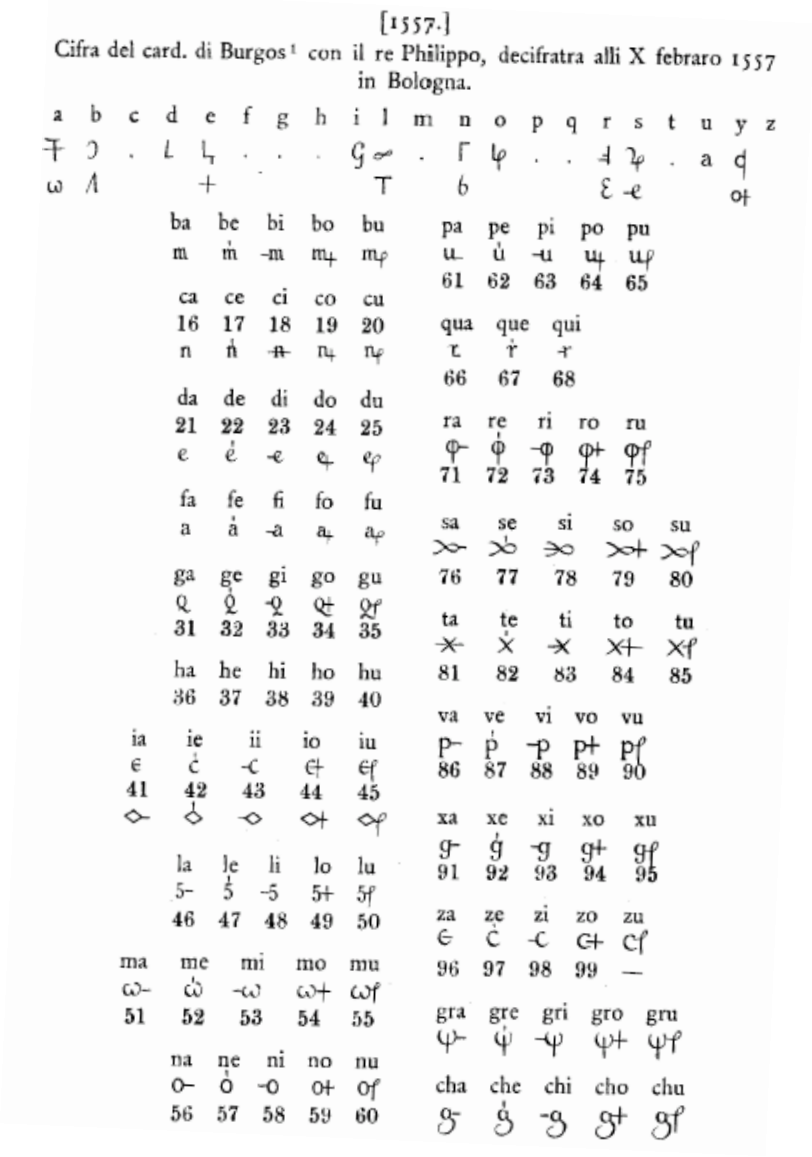


Figura 2.4
Nomenclátor de 1568 usado por Felipe II

IV. NOMENCLATOR 1557



[1557.]

Cifra del card. di Burgos[1] con il re Philippo, decifratra alli X febraro 1557 in Bologna.

a b c d e f g h i l m n o p q r s t u y z

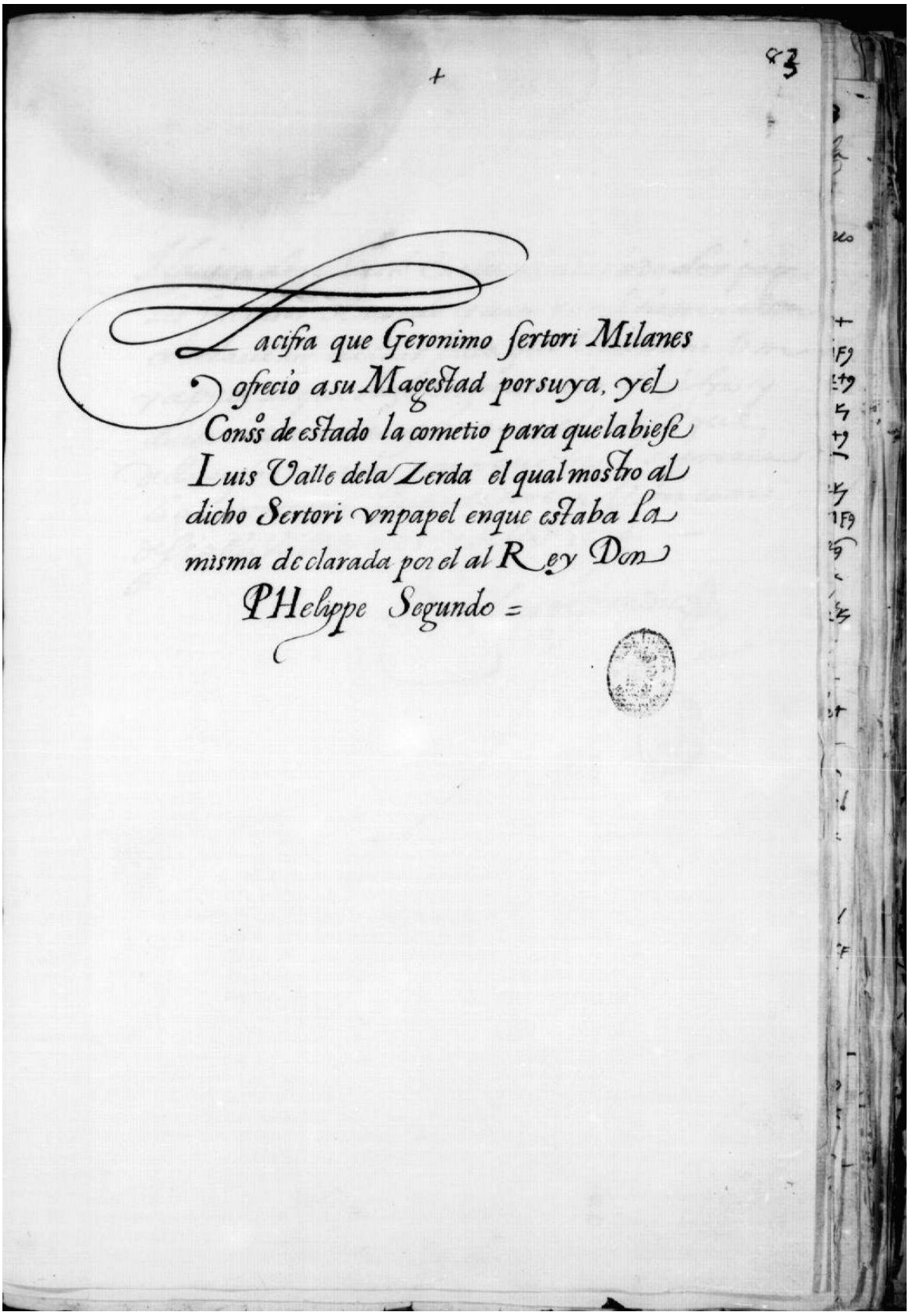
ω Λ + ⊤ b Ɛ ϵ ot

ba	be	bi	bo	bu	pa	pe	pi	po	pu
61	62	63	64	65					
ca	ce	ci	co	cu					
16	17	18	19	20	qua	que	qui		
66	67	68							
da	de	di	do	du					
21	22	23	24	25	ra	re	ri	ro	ru
71	72	73	74	75					
fa	fe	fi	fo	fu					
					sa	se	si	so	su
76	77	78	79	80					
ga	ge	gi	go	gu					
31	32	33	34	35	ta	te	ti	to	tu
81	82	83	84	85					
ha	he	hi	ho	hu					
36	37	38	39	40	va	ve	vi	vo	vu
86	87	88	89	90					
ia	ie	ii	io	iu					
41	42	43	44	45	xa	xe	xi	xo	xu
91	92	93	94	95					
la	le	li	lo	lu					
46	47	48	49	50	za	ze	zi	zo	zu
96	97	98	99	—					
ma	me	mi	mo	mu					
51	52	53	54	55	gra	gre	gri	gro	gru
					cha	che	chi	cho	chu
na	ne	ni	no	nu					
56	57	58	59	60					

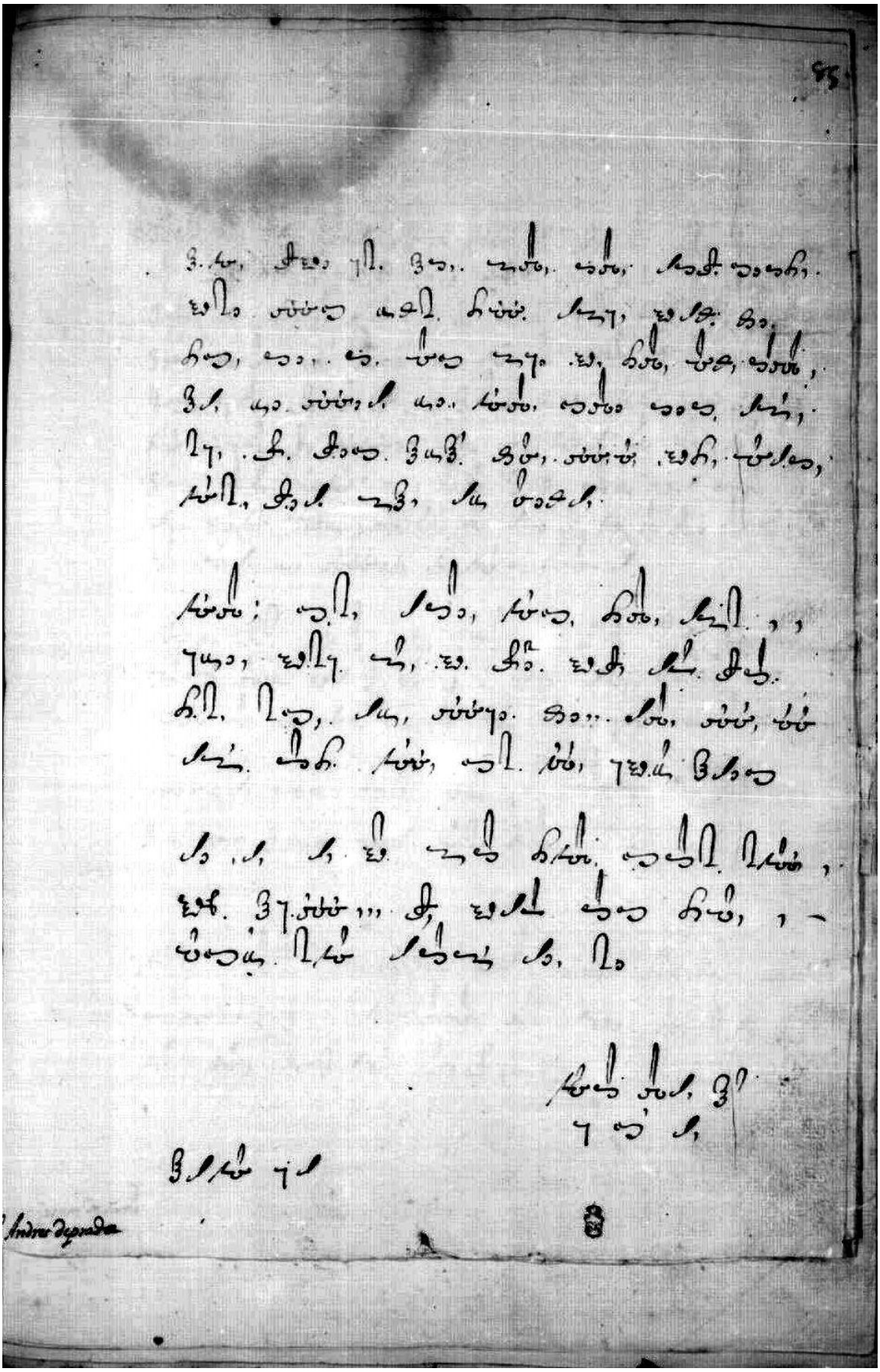
pra	pre	pri	pro	pru
tra	tre	tri	tro	tru

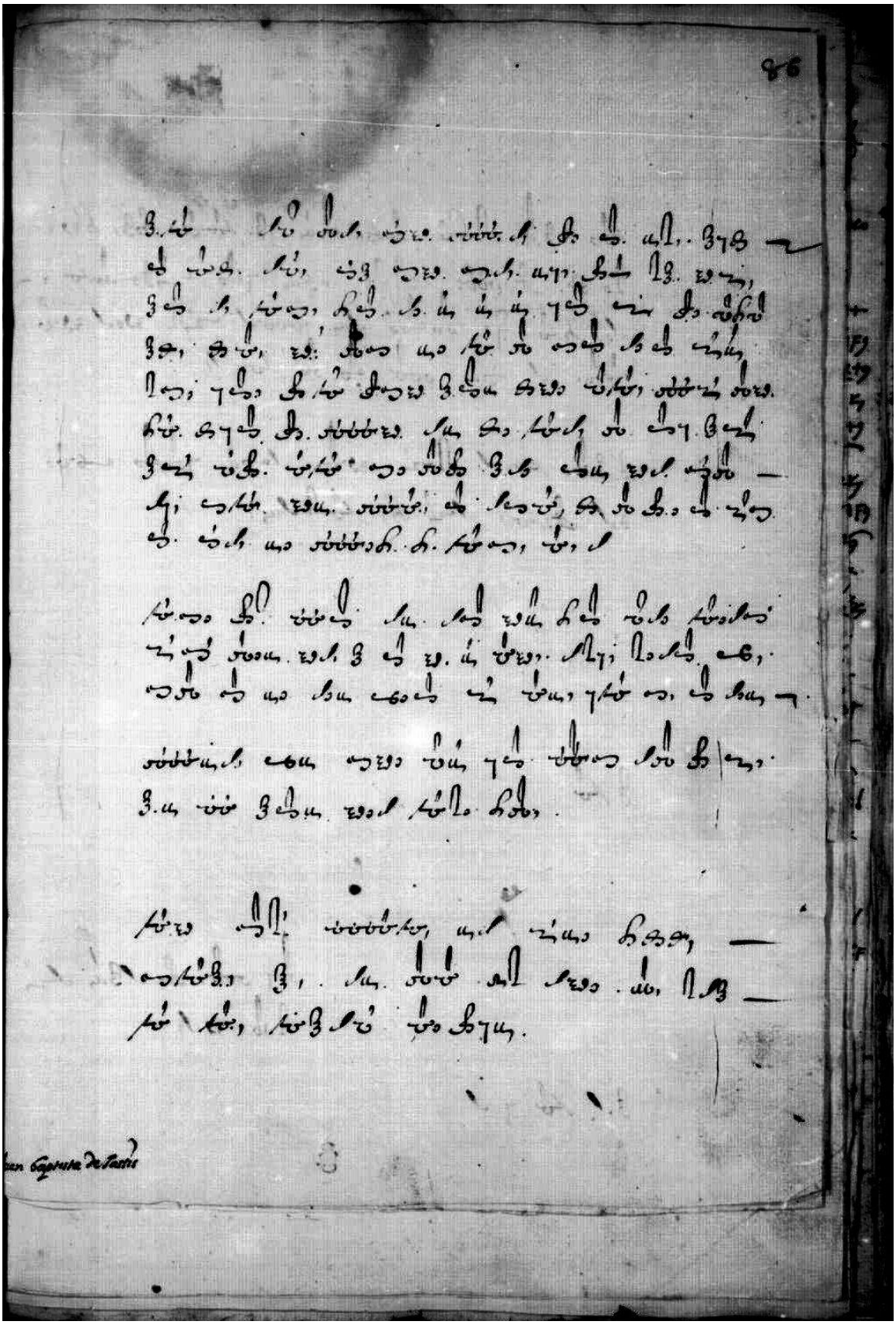
ff	ll	rr	ss	nn

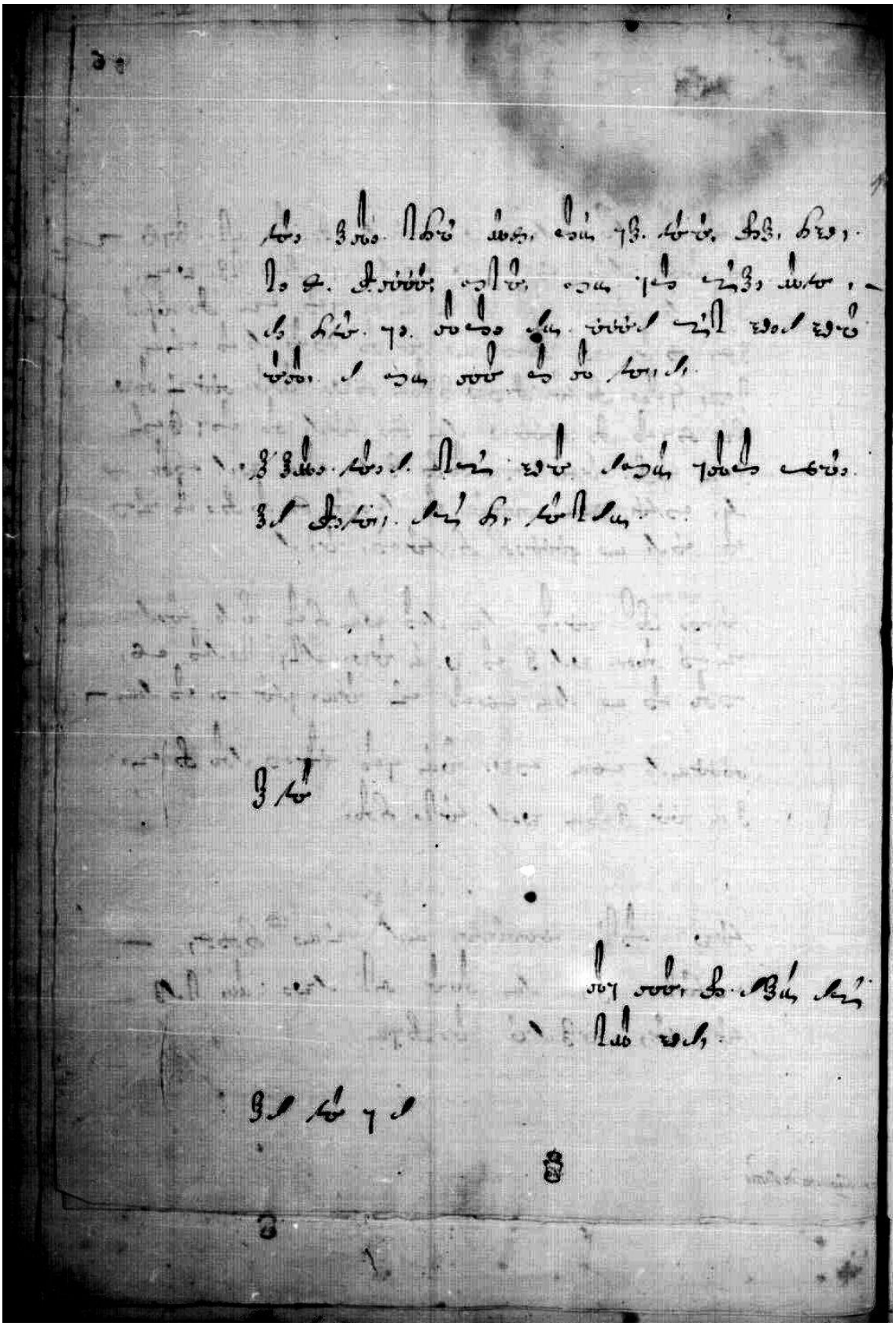
V. DOCUMENTO SERTORI (Siglo XVI)



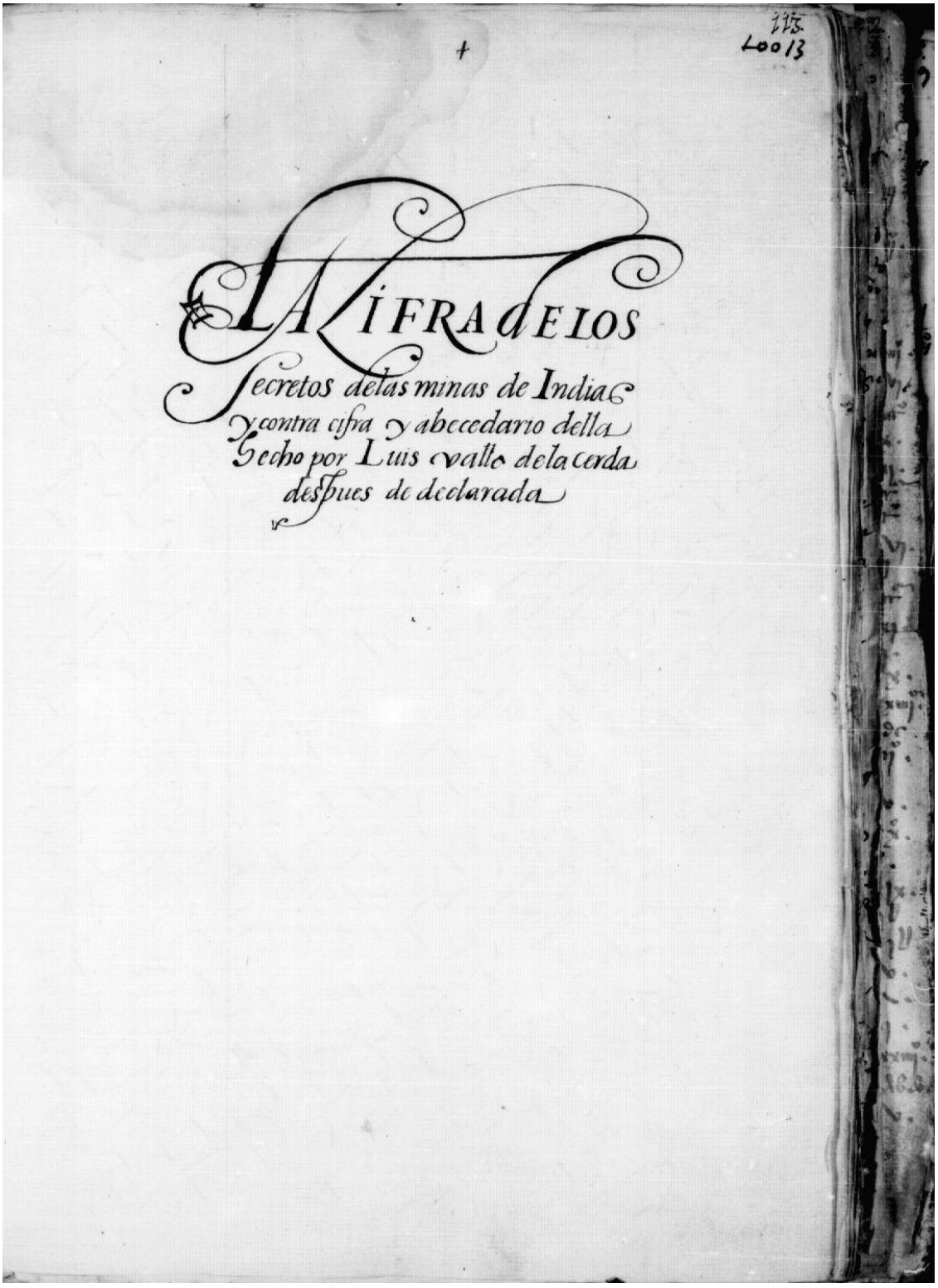
La cifra que Geronimo Sertori Milanes
ofrecio a su Magestad por suya, y el
Conss de estado la cometio para que la biese
Luis Valle dela Zerda el qual mostro al
dicho Sertori vn papel enque estaba la
misma declarada por el al Rey Don
PHelippe Segundo =

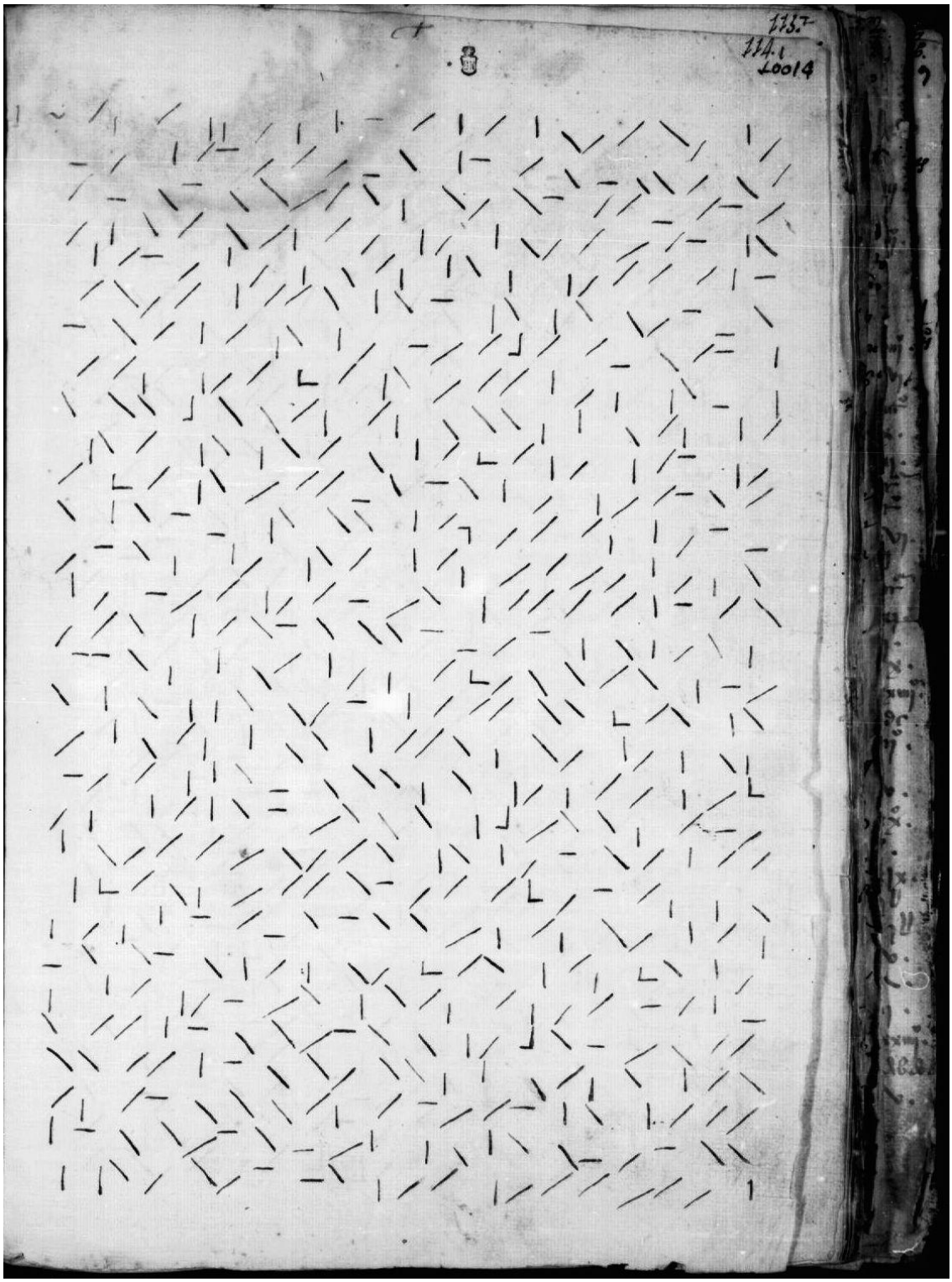


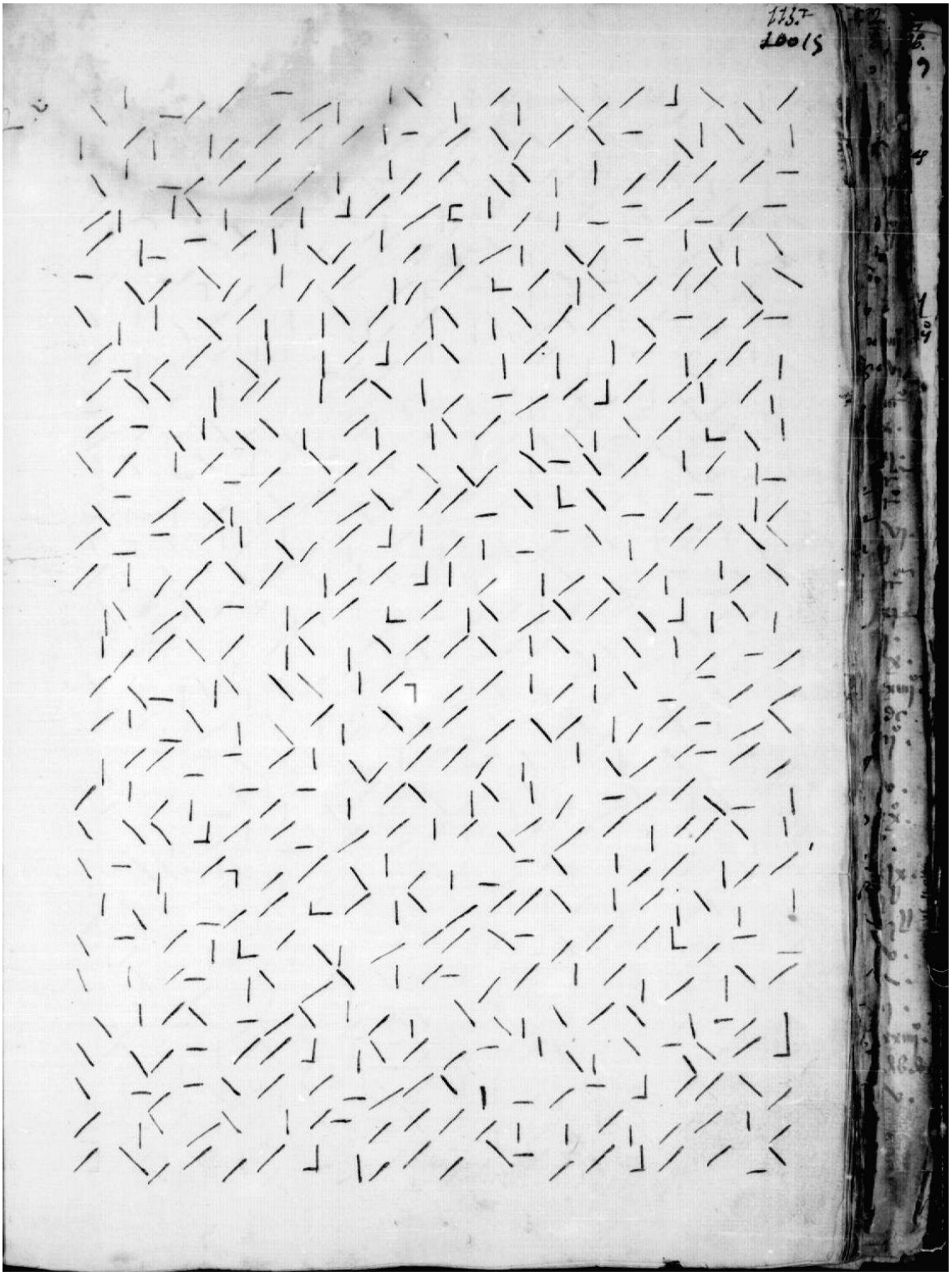




VI. DOCUMENTO MINAS (Siglo XVII)







VII. DOCUMENTO HISTÓRICO SIGLO XVII

EL

AIVSTAMIĒTO

I PROPORCION DE LAS
MONEDAS DE ORO, PLATA
I COBRE,

I

LA REDVCCION DESTOS METALES A
SV DEBIDA ESTIMACION,

SON

REGALIA SINGVLAR DEL REI DE
ESPAÑA, I DE LAS INDIAS, NVESTRO SEÑOR,
QVE LO ES DEL ORO I PLATA DEL ORBE,

Año de 1629.

AL REI N^RO S^OR

EL CAPITAN THOMAS DE CARDONA, MAESTRO DE SV CAMARA, I FISCAL EN LA REAL IVNTA DE MINAS.

SEÑOR.

DESDE el año de 1600. sin perdonar a trabajos i desvelos increibles, con no poca costa, insisto en el ajustamiento de las monedas de oro, plata i cobre, i en el aumento de las dos primeras, por diversos memoriales dados à V. M. (i antes al Rei D. Phelipe III. N.S. que està en el cielo) i por otros diversos papeles i discursos que he divulgado en su apoio, dando noticia delo que sobre pũto tan considerable con particular attencion he observado desde el año de 1580. que tuve edad competente para servir a V.M. cõ q̃ di principio a la milicia de mar i tierra, i navegaciones a las Indias. Las quales, i el manexo grande de los thesoros de oro i plata que vinieron desde aquel tiempo gran parte a mi cargo, como Maestre de plata de las naos de las armadas dela guarda de las Indias, Capitana i otras mias proprias, que vinieron en las armadas del cargo de don Francisco Coloma, i don Luis Faxardo, i otros, me fueron advirtiendo i mostrando su perjudicial desperdicio (causado del poco valor i estimacion que en España ha tenido el oro i plata, respeto de las demas naciones i Reinos circunvezinos) con perdida de mas de quinientos millones, que estos de V. M. han tenido, con utilidad de emulos, i enemigos desta Corona.